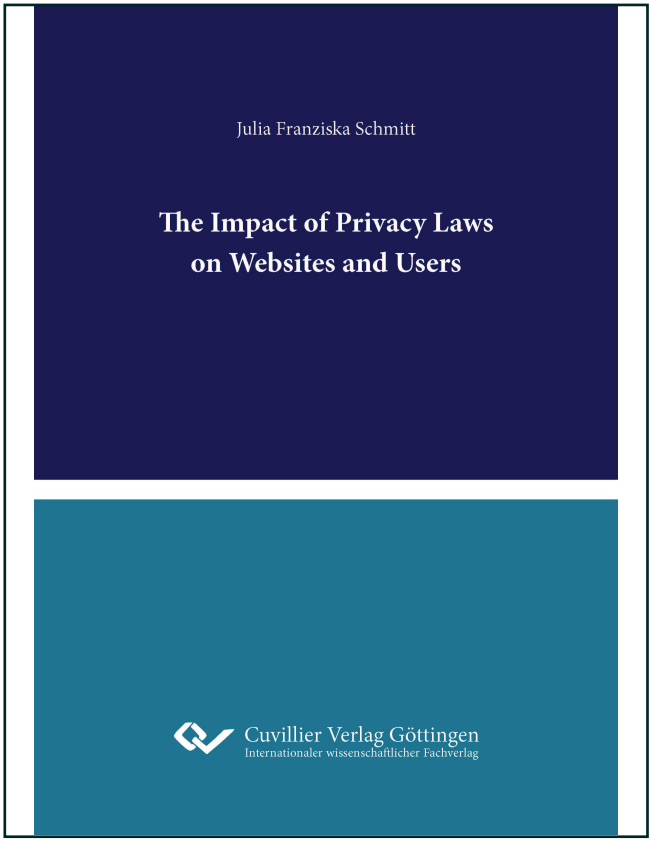
Julia Schmitt (Autor)

The Impact of Privacy Laws on Websites and Users



https://cuvillier.de/de/shop/publications/8623

0 Synopsis

0.1 Introduction

The collection and usage of users' personal data online has become crucial for companies and accelerates the tremendous growth of the digital economy (e.g., Reinsel et al. 2018). Websites benefit from collecting data about users by utilizing the data to personalize the user experience. For example, websites use the collected data about users to customize content and product recommendations and monetize the data by, e.g., enabling other firms to place targeted ads on the website (see, e.g., Skiera et al. 2021). Yet, the rapidly growing data collection on the internet fuels privacy concerns among users (Pew Research Center 2019) and strengthen the need for policymakers to regulate the data collection.

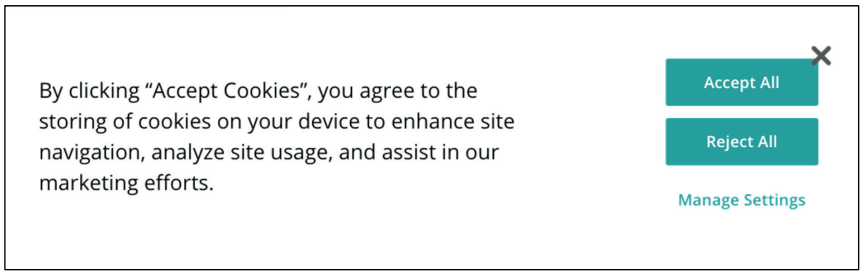
As a response to the privacy concerns, policymakers worldwide have enforced or are drafting new privacy laws such as the EU's General Data Protection Regulation (GDPR), Brazil's Lei Geral de Protecao de Dados (LGPD), Thailand's Personal Data Protection Act (PDPA), or India's Personal Data Protection Bill (PDPB). All these privacy laws aim to strengthen the protection and privacy of personal data and as a fundamental right (e.g., GDPR Recital 1 (2)). Increasing data privacy seeks to empower users to govern how companies use their personal data (e.g., GDPR Recital 7 (2)). Accordingly, policymakers, privacy laws as well as many practitioners and researchers follow Alan Westin's (1967) definition of privacy:

"the claim of individuals […] to determine for themselves when, how, and to what extent information about them is communicated."

This definition, the common definition of privacy, builds upon the users' control over their personal data – and lays the foundation for the idea that consent is the key to providing users with more privacy. Thus, privacy laws strongly focus on providing users with the ability to consent to the usage of their personal data. For example, for the use of online tracking technologies, policymakers require websites to obtain the users' consent via an opt-in approach (regulated in GDPR Art. 7; LGPD Art. 5 XII; PDPA Section 19; PDPB Section 11 (2); reinforced by, e.g., Curia 2019). Obtaining consent via an opt-in approach, also known as explicit consent, means that a user must actively accept the data collection and usage on a website. Per default,

i.e., if the user does not take any action on a consent request, the user denies consent. Commonly, to request the users' consent and to inform users about the websites' data usage, websites display so-called consent banners to users (see Figure 0.1 for an example of a consent banner).

Figure 0.1: Example of a Consent Banner



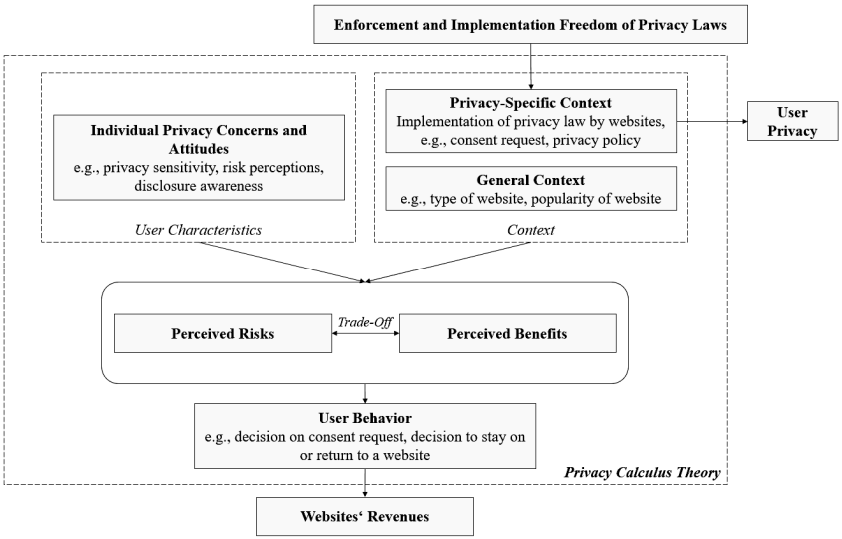
While the means to request consent from users is the same across websites, i.e., a consent banner, policymakers decided to give websites the freedom of choosing how they design consent banners while staying within the legal boundaries (see, e.g., GDPR Recital 32). With websites being relatively free in the specific implementation of the design of these consent banners, websites implemented the same requirements for consent in various ways (e.g., Degeling et al. 2019, Sanchez-Rola et al. 2019). Policymakers within the privacy law GDPR further fuel these differences in consent banner designs across websites by issuing inconsistent official guidelines within the scope of the same privacy law. For example, the data protection authority (DPA) in Spain regards consent as valid when the users keep browsing the website if the website informs the users of the consequence of their behavior (AEDP 2019). In contrast, the French DPA does not consider consent to be valid if the users simply keep browsing the website (CNIL 2019).

Currently, it is unclear how the degree of freedom that policymakers grant websites in the implementation of consent banners and the resulting differences in consent banners affect websites and user privacy. Yet, when drafting privacy laws, policymakers have to trade-off between increasing user privacy and damaging websites economically by restricting their ability to collect personal data and, therefore, to monetize it. If the implementation freedom affected this trade-off, e.g., design differences in consent banners affected user privacy or the websites'

ability to earn revenue, such effects would be crucial for policymakers to consider when evaluating privacy laws. Similarly, websites would need to account for the effect of design differences to optimally decide upon a design to implement.

Indeed, research suggests that design differences in privacy settings can impact privacy and the user behavior. More specifically, the privacy calculus theory (Dinev and Hart 2006) proposes that user behavior in privacy settings is a result of a trade-off that users conduct. In this trade-off, the user weights the perceived losses, e.g., data breaches, and perceived gains, e.g., better content suggestions, of a privacy decision against each other. The theory further proposes that the result of this trade-off depends on the users' individual privacy concerns and attitudes as well as the context of privacy decisions. This second aspect, the context of privacy decisions, encompasses both the general characteristics of websites, e.g., website industry and popularity, and the websites' specific implementation of privacy options, e.g., the design of a consent request or privacy policy. Consequently, as Figure 0.2 visualizes, the privacy calculus theory suggests that the specific implementations of privacy laws and consent banners resulting from the implementation freedom of privacy laws affect user behavior.

Figure 0.2: Theoretical Foundation of Dissertation



For websites, the potential effect of the implementation freedom of privacy laws on user behavior can be an opportunity: Websites can use the freedom to optimize the design of the consent banner and the implementation of other legal requirements. However, it also poses challenges for websites. Firstly, the freedom increases the existing uncertainty about whether a specific implementation is compliant due to the ample design space and conflicting official guidelines. Thus, considering the legal requirements imposed by privacy laws and official guidelines issued by data protection authorities becomes even more challenging for websites as a result of the implementation freedom. Secondly, websites must carefully consider how potential implementations of consent banners and other legal requirements will affect user behavior on their website.

For example, different implementations of privacy laws on a website might affect 1) the probability that users consent to a website's data usage (the so-called "consent rate"), 2) the users' decision to stay on a website, or 3) the users' decision to return to a website. Suppose an ad-financed website that earns revenue from displaying ads to users chose an implementation that negatively impacted these three decisions for its user base. Consequently, the website would obtain the users' consent for fewer users, resulting in the website being able to personalize the displayed ads for fewer users, reducing the ads' and, ultimately, the websites' profitability. Additionally, the users may leave the website sooner and re-visit the website less often, i.e., interact less with the website, resulting in the users seeing fewer ads on the website. Consequently, the reduced ad profitability and reduced number of ads shown to the users would diminish the ad-financed website's revenue.

Despite research indicating an effect of different implementations of privacy laws, e.g., the specific design of consent banners, on user behavior, no knowledge exists about this effect. Consequently, websites cannot anticipate whether and how the implementation of privacy laws affects user behavior and, thus, their revenues. Yet, websites must assess the effect that different privacy law implementations and different consent banner designs have on user behavior as a driver of their revenues to adequately choose how to implement privacy laws. For this endeavor, websites need an empirical foundation.

Similarly, to best assess existing privacy laws and to draft future ones, policymakers need to evaluate whether existing privacy laws achieved their aim to increase user privacy while not

strongly damaging websites. As described above, the privacy calculus theory implies that different implementations of the same legal requirements can affect websites' revenues (see Figure 0.2). Accordingly, the empirical foundation about the effect of different privacy law implementations on user behavior can aid policymakers when evaluating the economic damage that privacy laws cause to websites.

Furthermore, the different implementations can affect the level of privacy that users have on websites. More specifically, the privacy calculus theory highlights that user privacy and the user decision in privacy settings depends on, amongst others, the 1) availability of privacy options and 2) convenience of selecting the privacy options (Ajzen 1991; Dinev and Hart 2006) as users are convenience-driven (e.g., Anderson 1972). Thus, the privacy calculus theory indicates that the implementation freedom of privacy laws affects user privacy if the freedom results in websites implementing the same requirements differently in terms of availability and convenience. Yet, existing research investigating GDPR's effect on user privacy (e.g., Degeling et al. 2019) only focuses on the first aspect, the availability of privacy options.

Consequently, there is a lack of knowledge about whether and how privacy laws and the differences in the implementation of the legal requirements, such as the consent requirement, affect websites' revenue and user privacy. This lack of knowledge prohibits policymakers from thoroughly examining whether privacy laws and the implementation freedom achieved their aim to limit the damage to websites while increasing user privacy. Thus, policymakers need an empirical foundation that aids them in assessing whether current privacy laws need additional specifications and that enables them to apply this knowledge in the drafting stage of future privacy laws.

0.2 Aim and Structure of Dissertation

This dissertation aims to shed light on the effects of privacy laws and their implementation freedom on 1) websites' revenues and 2) user privacy. To investigate the effects of privacy laws on websites' revenues and user privacy, this dissertation uses the enforcement of the privacy law GDPR to examine its effects on websites and users. The articles included within this dissertation further provide insights into the impact of the implementation freedom for consent banners on websites' revenues and user privacy.

To assess the privacy law's effect on websites' revenues, I examine the websites' user quantity and quality as an indicator of the websites' ability to earn revenue, e.g., via product sales or ads. To assess the privacy law's effect on user privacy, I examine the control that users have over their personal data and the convenience of that control (see Figure 0.3) in the post-GDPR era.

For these purposes, this dissertation includes three articles that investigate different factors that influence websites' revenues and user privacy using statistical methods and novel datasets. Figure 0.3 shows the different factors that influence websites' revenues and user privacy and visually outlines which article addresses which factors.

Table 0.1 summarizes the details of the three articles. Specifically, in Article I, I examine the GDPR's effect on websites' revenue in terms of user quantity and user quality measured by the usage intensity. In Article II, I examine the GDPR's effect on websites' revenue in terms of the user quality measured by the consent rate. Finally, in Article III, I examine the user privacy post-GDPR regarding the control and convenience of the privacy options.

Figure 0.3: Aim of Thesis and Scope of Articles

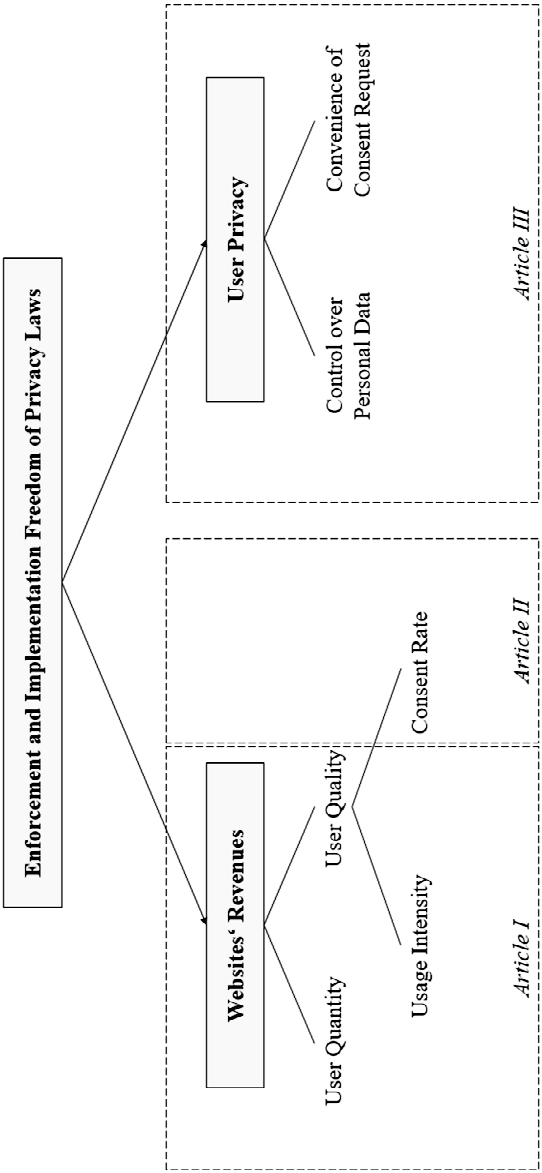


Table 0.1: Description of Articles within Thesis

	Article	Research Aims	Dataset	Applied Methods	Results	Status
I	The Impact of Privacy Laws on User Behavior *Julia Schmitt, Klaus Miller, Bernd Skiera*	• Examine the effect of websites' implementation of GDPR on user behavior over time • Investigate how effects vary based on website and user characteristics	• Weekly traffic data on five user behavior metrics over 2.5 years • Scraped website location data • 6,286 websites (Top 1,000 of 14 countries) across 24 industries	• Empirical Study: Enforcement of GDPR • Synthetic Control Group Method • Panel Difference Estimator; Regression • Mean Comparisons / t-test	• On average, GDPR affected user quantity and usage intensity negatively • Effect stronger over time • Effects vary across websites • Website popularity and industry are strong indicators of effect size and direction	Under 2nd Round Review at the *Journal of Marketing Research*
II	Choose Wisely: The Impact of Consent Banner Designs on Consent Rates *Julia Schmitt*	• Examine whether consent banners' characteristics affect consent rate • Quantification of effects • Investigate how websites can take advantage of freedom to increase consent rate compliantly	• Two datasets from field experiments with Consent Management Provider • User-level data on consent decision	• Field Experiments: Variation of consent banners • ANOVA	• Characteristics have significant effects on consent rate • Change of consent rate between 1.60 and 14.90 percentage points per characteristic • Determination of combination of characteristics that increases consent rate for websites	Working Paper
III	The Illusion of Control: Control and Convenience on Consent Banners *Julia Schmitt*	• Examine theoretical and practical distribution of consent banners' control and convenience • Examine relationship of consent banners' control and convenience • Examine whether and how consent banners can be more convenient	• Data on user preferences • Manually collected set of consent banner designs on 1,850 websites (Top 500 websites of five countries)	• Empirical Study: Manual collection of consent banner designs • In-depth interviews • Conjoint Analyses • Hierarchical Bayes Model	• Websites offer high control at cost of convenience • Consent banners with one layer lack control; consent banners with two layers lack convenience • Maximization of control and convenience possible	Working Paper

0.3 Summary and Results of Articles

The first article (Chapter 1) examines the effect of GDPR on user behavior on websites over time. Specifically, the article captures user behavior in terms of user quantity (e.g., total number of visits) and user quality in terms of usage intensity (e.g., page impressions per visit). Both the user quantity and usage intensity can impact the websites' revenue, as outlined above. Furthermore, different implementations of GDPR across websites can affect user behavior differently. For example, different implementations of GDPR's requirements across websites could include differences in consent banner designs, privacy policies, or the websites' ability to personalize the user experience to engage users better. Accordingly, the article further examines how the GDPR's effect varies across websites and as a function of website and user characteristics.

The article utilizes a dataset containing weekly traffic data for the Top 1,000 websites of 12 EU countries as well as the US and Switzerland. Overall, the analysis includes traffic data for 6,286 unique websites across 24 industries. The traffic data encompasses five user behavior metrics (total number of visits, number of unique visitors, number of page impressions, total visit duration, number of bouncing visitors) from July 1st, 2017, to November 30th, 2019. Thus, the weekly traffic data is available for almost a year prior to the enforcement of GDPR and captures the effect of GDPR on user behavior over 1.5 years.

To examine the GDPR's effect on user behavior, we use the enforcement date of GDPR, May 25th, 2018, as the event for our empirical study. To draw inferences on the impact of GDPR coming into effect, we further consider the GDPR's scope peculiarities and combine a synthetic control group (SCG) approach with a panel difference estimator, similar to a Difference-in-Differences (DiD) analysis. First, we calculate the GDPR's effect on each website, enabling a detailed investigation of the distribution of GDPR's effects across our website sample. We then use the results on the website level to examine how the GDPR's effects vary based on website and user characteristics (i.e., website industry and popularity; user country of origin).

We find that GDPR affects websites in one of two major ways: Some websites have difficulties attracting the same amount of users as before GDPR (i.e., GDPR negatively affects the user quantity), while other websites face difficulties engaging users the same way as before

GDPR (i.e., GDPR negatively affects the usage intensity). Regarding the user quantity, GDPR harms websites, on average, and the negative effect becomes stronger over time. For example, the total number of visits to a website dropped by, on average, 4.90% after 3 months and 10% after 18 months of GDPR. However, the websites that experience decreased user quantity benefit in terms of usage intensity and vice versa. For example, after 18 months of GDPR, the websites that experience decreased total visits experience an increase in the page impressions per visit by 5.53%.

The article further shows that the GDPR's effects across websites differ strongly in size and direction, with some websites even benefiting from GDPR. Both the effect direction and sizes vary across website popularity, website industry, and user country of origin. Most notably, less popular websites experience even more negative effects than popular ones, suggesting an increased market concentration after GDPR.

The most prominent change on the websites' user interface after the enforcement of GDPR is their adjustment of the consent banner. While there are other aspects that websites had to adjust, e.g., the privacy policy, the first interaction that users have on a website is their interaction with the consent banner. Thus, although Article I does not specifically investigate how the websites implement the consent banner, the difference in the GDPR's effects likely stem – at least to some extent – from different consent banner implementations. To investigate this aspect further, the subsequent articles specifically focus on the effect of implementation differences of consent banners.

The second article (Chapter 2) examines the effect of differences in consent banners on user quality in terms of the consent rate, i.e., the share of users accepting the data collection and usage on a website. Websites can vary the design of consent banners while considering legal regulations and official guidelines, resulting in a sizeable possible design space. The second article aims to examine whether and how changing the characteristics of consent banners affects the user quality in terms of the consent rate and to quantify the effects. The article further shows how websites can use the determined effects of consent banner characteristics to take advantage of the vast design space to increase the consent rate compliantly.

To achieve the described aim, I conduct two field experiments with a large international consent management provider (CMP). A CMP supports websites in the technical implementation of consent banners and the subsequent recording and management of the users' consent