Article

How Do Privacy Laws Impact the Value for Advertisers, Publishers and Users in the Online Advertising Market? A Comparison of the EU, US and China

Journal of Creating Value
8(2) 306–327, 2022

DOI: 10.1177/23949643221117676
journals.sagepub.com/home/jcv

Yuxi Jin[1] and Bernd Skiera[1,2]

Abstract

Regulators worldwide have been implementing different privacy laws. They vary in their impact on the value for advertisers, publishers and users, but not much is known about these differences. This article focuses on three important privacy laws (i.e., General Data Protection Regulation [GDPR], California Consumer Privacy Act [CCPA] and Personal Information Protection Law [PIPL]) and compares their impact on the value for the three primary actors of the online advertising market, namely, advertisers, publishers and users. This article first compares these three privacy laws by developing a legal strictness score. It then uses the existing literature to derive the effects of the legal strictness of each privacy law on each actor's value. Finally, it quantifies the three privacy laws' impact on each actor's value. The results show that GDPR and PIPL are similar and stricter than CCPA. Stricter privacy laws bring larger negative changes to the value for actors. As a result, both GDPR and PIPL decrease the actors' value more substantially than CCPA. These value declines are the largest for publishers and are rather similar for users and advertisers. Scholars and practitioners can use our findings to explore ways to create value for multiple actors under various privacy laws.

[1] Department of Marketing, Faculty of Economics and Business, Goethe University Frankfurt am Main, Germany
[2] Deakin University, Melbourne, Australia

Corresponding author:
Bernd Skiera, Goethe University, Theodor-W.-Adorno-Platz 4, Frankfurt 60629, Germany.
E-mail: skiera@wiwi.uni-frankfurt.de

Keywords
GDPR, CCPA, PIPL

Received 7 June 2022; **accepted** 7 June 2022

Introduction

Regulators worldwide enact various privacy laws to alleviate users' privacy concerns about firms' intensive processing of personal data. These privacy laws regulate personal data processing by imposing obligations on firms and entitling users with rights, potentially impacting the value for firms (e.g., by raising costs) and users (e.g., by increasing utility from higher privacy). The impact of privacy laws on the value created in the online advertising market is likely to be substantial because firms operating in this market rely heavily on personal data processing to provide users with personalized offerings (Skiera et al., 2022).

Understanding how privacy laws affect value is a critical task for firms because they need to create (or at least prevent from destructing) value for multiple stakeholders, especially under policy shocks such as the enforcement of privacy laws (Kumar & Rajan, 2017; Kumar & Reinartz, 2016). Such knowledge is also important for users because they need to understand the consequences they may encounter (e.g., less relevant ads and more privacy choices) and how laws protect their privacy. In particular, this article focuses on three primary actors in the online advertising industry: advertisers, publishers and users.

However, it has been challenging to understand how different privacy laws affect value because little is known about the differences between the laws and how they impact each actor's value in the online advertising market. Therefore, this article examines the privacy laws of three important regions worldwide, namely, the General Data Protection Regulation (GDPR) in the European Union (EU), the California Consumer Privacy Act (CCPA) in an essential part of the United States (US) and the Personal Information Protection Law (PIPL) in China, to derive their effects on the value for actors in the online advertising market—advertisers, publishers and users. Our study is the first to compare the three privacy laws simultaneously and to bring China's PIPL into the discussion.

This article adopts the method of theory synthesis (Jaakkola, 2020) that summarizes and integrates existing knowledge of a concept or phenomenon, which, in our context, is the creation and destruction of value by privacy laws. In the first step, we use a set of criteria to create a *legal strictness score* for each of the three laws to derive their similarity. In the second step, we provide an overview of the effects of legal strictness on the value for the actors affected. Specifically, we examine the exchanges between advertisers, publishers and users to (a) define the value for one actor by another actor (e.g., the value created or destroyed for users by publishers), (b) examine the existing literature to describe the effects of privacy laws on value and (c) quantify the total effects of legal strictness for each actor by adding up all effects on value—*sum of effects on value*. Thus, we add to

the understanding of value creation and destruction from multiple stakeholders' perspectives in the context of privacy laws and the online advertising market.

In the third and final step, we derive the *changes in value* by multiplying the *legal strictness score* and the *sum of effects on value* that yield the effects that each privacy law has on each actor. We provide a method to quantitatively summarize different laws' effects on the value for multiple actors, allowing for detailed conclusions for each law and actor.

Existing Knowledge of Value and Privacy

Our study contributes to two streams of the literature. First, we offer a systematic overview of how privacy laws affect the value for firms and users. Many studies investigate the effects of privacy laws with a focus on one actor: publishers (e.g., Congiu et al., 2022), advertisers (e.g., Johnson et al., 2022) or users (e.g., Ichihashi, 2020). Few articles discuss multiple actors, but they do not shed light on the combined effects of the multiple mechanisms through which privacy laws change the value for actors (Johnson et al., 2020). Meanwhile, many discussions on consumer privacy concentrate on the GDPR in the EU, neglecting other privacy laws such as the CCPA and the PIPL (Aridor et al., 2020; Goldberg et al., 2021; Schmitt et al., 2021).

Second, this article adds to the understanding of value creation in the context of privacy. Kumar and Reinartz (2016) discuss value in the exchanges between firms and customers. They define the perceived value for customers and measure the value from customers. Kumar and Rajan (2017) define value for firms from a stakeholder's (e.g., customers, employees and investors) perspective and explain how stakeholders create or destroy value for firms. Nevertheless, there is a gap in understanding value creation and destruction for multiple stakeholders. Our study bridges the gap by examining the exchanges between publishers, advertisers and users and providing a detailed description of how these exchanges create or destroy value.

Comparison of the Three Privacy Laws

Overview of the Three Privacy Laws

We compare three privacy laws from important regions of the world: (a) the GDPR in the EU, (b) the CCPA in California in the US and (c) the PIPL in China. As top economies worldwide (measured by Gross Domestic Product), the EU (third), California (fifth) and China (second) have privacy laws that are likely to have a considerable impact on value for all actors. Meanwhile, the three areas have wide regional coverage, each representing a different continent.

Criteria for Comparison

We adopt the 5W1H method to develop the criteria for deriving the *legal strictness score* of the three privacy laws. The 5W1H method describes a situation with six dimensions: where, when, why, who, what and how. Adopting the method allows for better understanding, structuring and framing of a situation (Carmagnola, 2008). Specifically,

- Scope (where): It describes the applicable activities, the protected actors and the regulated actors of the law.
- Time of enforcement (when): It describes when the law takes effect.
- Aim (why): It describes the aim of the law.
- Role of the regulated firms (who): The role distinguishes the regulated actors by (a) firms determining why and how to process data and (b) firms processing data for the actors in (a).
- Definition of data to be protected (what): The applicable data is categorized into (a) the data generally protected and (b) the data protected by special rules.
- Legal bases, user rights, firm obligations and penalties (how): Each describes a key component of the laws to protect user privacy—the legal bases a law requires for data processing, the rights a law entitles users with, the obligations a law imposes on a firm and the penalties a law enforces.

Methodology for the Comparison of the Three Privacy Laws

Table 1 presents a comparison of the three privacy laws. Each column of Table 1 contains one of the three privacy laws, and the rows display the criteria used for our comparison. We fill the cells with integrated information from law articles and industry reports (Jehl & Friel, 2018; Kulbeth, 2021; Marini et al., 2018).

To draw conclusions based on quantitative evidence, we (a) develop a *legal strictness score*, (b) summarize each law's legal strictness and (c) check the similarities and differences between the laws in Table 2. Specifically, the *legal strictness score*, ranging from 0 to 2, is based on the relative ranking of legal strictness among the three laws, that is, we assign the highest score of '2' to the law ranking the first in legal strictness ('1' for the second and '0' for the third). Our evaluation of a higher ranking in legal strictness differs for each criterion: broader scope, earlier enforcement time, more aims to achieve, more roles of the regulated firms, broader definition of data to be protected, more legal bases, more user rights, more firm obligations and higher penalties.

When two laws are equally strict in a criterion, they get the same score. Take the criterion scope as an example. The GDPR and the PIPL have an extraterritorial scope, while the CCPA mainly applies to California. Hence, the GDPR and the PIPL tie at the first rank, having a *legal strictness score* of '2', while the third-placed CCPA scores '0'. For the criteria where the three laws are equally strict, all get the highest score of '2' as the *legal strictness score*.

Table 1. Comparison of the Three Privacy Laws (GDPR, CCPA and PIPL).

		GDPR	CCPA	PIPL
Scope (where)	Regulated Firms	• EU firms (controllers/processors) • Non-EU firms, when providing products to users in the EU or analysing activities of users in the EU	California firms ('businesses'), when satisfying one of the following conditions • Annual gross revenue over $25 Mio • Collect/sell/buy/share data of over 50,000 consumers for commercial purposes • More than half of the annual revenue from selling data	Firms that process personal data • In China • Outside of China, when providing products to users in China or analysing activities of users in China
	Protected persons	Natural persons whose personal data is processed • In the EU • By EU firms	Natural persons who are California residents	Natural persons whose personal data is processed in China
	Activities of the regulated firms to the protected persons	Personal data processing (any operation)	Personal data collection, selling or sharing	Personal data processing (any operation)
Enforcement time (when)		25 May 2018	1 January 2020	1 November 2021
Aim (why)		Protect user right of personal data	Protect user right of personal data	Protect user right of personal data
Role of the regulated firms (who)	Determine the purposes and means of data processing	Data controllers	Data controllers ('businesses', with many extra conditions)	Data controllers ('personal information handling entity')
	Process data on behalf of others	Data processors (with several obligations)	Data processors ('service providers')	Data processors ('entrusted persons')
Definition of protected data (what)	General	Personal Data: Any information related to identified or identifiable natural persons	Personal Data: Any information related to identified or identifiable natural persons Exemptions of • Personal health information (PHI) • Financial Information	Personal Data: Any information related to identified or identifiable natural persons

(Table 1 continued)

(Table 1 continued)

		GDPR	CCPA	PIPL
	Protected by special rules	Biometric Religious beliefs Medical health Racial or ethnic origin Political opinion Trade union membership Sex life or sexual orientation	NA	Biometric Religious beliefs Medical health Financial accounts Location Minors
Legal bases (how)	Consent	Yes (opt-in)	No (except opt-out for selling data)	Yes (opt-in, separate opt-in for sensitive information)
	Legitimate interest	Yes	No	No
	Contract fulfilment	Yes	No	Yes
	Legal requirement	Yes	No	Yes
	Vital interest	Yes	No	Yes
	Public interest	Yes	No	Yes
	Disclosed Information	No	No	Yes
User rights (how)	Information	Yes	Yes	Yes
	Access	Yes	Yes	Yes
	Correction	Yes	No	Yes
	Erasure	Yes	Yes	Yes
	Data portability	Yes	Yes	Yes
	Object/restrict processing	Yes	No (except opt-out for selling data)	Yes
	Quit automated decision-making	Yes	No	Yes
	Withdraw consent	Yes	No	Yes
	Lodge a complaint	Yes	No	Yes
	Non-discrimination	No	Yes	No

(Table 1 continued)

(Table 1 continued)

		GDPR	CCPA	PIPL
Firm obligations (how)		Data controllers and data processors should: • Process personal data based on a legal basis • Document personal data processing activities • Implement technical and organizational measures • Conduct Data Protection Impact Assessment • Notify personal data breaches • Appoint a Data Protection Officer Data controllers (not processors) should: • Select the purposes of personal data processing • Justify the relevance of personal data • Assure the compliance of their data processors	Data controllers should: • Inform consumers of the categories and purposes of data collection • Delete a consumer's personal data upon request • Notify consumers and provide a way to opt-out when selling their personal data to third parties • Not discriminate against a consumer for exercising their rights (e.g., deny goods or services, charge different prices)	Data controllers should: • Process personal data based on a legal basis • Implement technical and organizational measures • Conduct a prior personal information protection impact assessment and keep a record (≥ 3 years) • Notify personal data breaches and adopt remedial measures • Appoint a Personal Information Protection Officer • Establish a dedicated entity or appoint a representative inside China for those firms outside of China • Audit the compliance with the laws regularly • Extra obligations for those impactful
Penalties (how)	Less serious violations of law	Up to $11 Mio or 2% worldwide annual revenue (whichever is larger)	Up to $2,500 (if a firm fails to cure the violation after a 30-day notification)	Firm: Up to $150,000 Person in charge: $1,500–$15,000
	More serious violations of law	Up to $23 Mio or 4% worldwide annual revenue (whichever is larger)	Up to $7,500 (if a firm fails to cure the intentional violation after a 30-day notification)	Firm: Up to $8 Mio or 5% annual revenue Person in charge: $15,000–$150,000 & prohibition of holding a high position

Source: The authors.

Table 2. Legal Strictness for the Three Privacy Laws (GDPR, CCPA and PIPL).

Criterion ID	5W1H	Criteria	Legal Strictness Score[a] (Scale: 0–2)			Similarity of Law Legal Strictness[b] (Binary: 0 or 1)		
			GDPR	CCPA	PIPL	GDPR = CCPA	CCPA = PIPL	GDPR = PIPL
1	Where	Scope	2	0	2	0	0	1
2	When	Enforcement time	2	1	0	0	0	0
3	Why	Aim	2	2	2	1	1	1
4	Who	Role of regulated firms	2	2	2	1	1	1
5	What	Definition of data to be protected	2	0	2	0	0	1
6	How	Legal bases	2	0	2	0	0	1
7		User rights	2	0	2	0	0	1
8		Firm's obligations	2	0	2	0	0	1
9		Penalties	2	0	2	0	0	1
Total			18	5	16	2	2	8

Source: The authors.

Notes: [a]The ranking of legal strictness of the three laws yields the legal strictness score, that is, the strictest law gets the highest score of '2' ('1' for second and '0' for third strictest law).
[b]We fill the cells with '1' if the respective two laws are equally strict and 0 otherwise.

Then, we check the similarity conditions regarding legal strictness according to the *legal strictness score*. For example, when checking 'GDPR = CCPA' under the criterion 'where', we see whether '0 = 2' holds. Since the equality is false, the cell contains '0'.

Results of the Comparison of the Three Privacy Laws

We observe in Table 2 that the GDPR and the PIPL are similar in their legal strictness, based on the considerable overlap of eight out of nine criteria. The *legal strictness score* can also support the conclusion as the GDPR has a total score of 18 while the PIPL scores 16 in legal strictness. Both laws have an extraterritorial scope and protect certain sensitive data with special rules. Besides, the two laws require firms to support data processing with analogous legal bases, share one set of analogous user rights and punish serious violations with fines up to millions (even billions) of dollars.

In addition, we find the CCPA is less strict than the GDPR and the PIPL (*legal strictness score*: $5_{CCPA} \ll 16_{PIPL} \approx 18_{GDPR}$). First, the CCPA has a narrower scope than the other two laws: (a) collecting, selling or sharing versus any operation, (b) California residents versus natural persons and (c) California firms ('businesses') under certain conditions versus explicit extraterritorial long arm. Second, the CCPA has a narrower definition of data to be protected. In particular, certain health and finance data is exempted from protection under the CCPA but is protected with even stricter rules under the other two laws. Third, the CCPA entitles fewer user rights than the GDPR and the PIPL. Last but not least, the CCPA imposes penalties of a smaller scale than the other two laws, let alone the PIPL's additional punishment on the person in charge.

Despite their comparable *legal strictness scores*, there are distinctions between the GDPR and the PIPL, and both can be stricter than the other one under specific criteria. On the one hand, the PIPL can be stricter than the GDPR. Apart from most shared legal bases, the PIPL does not support using legitimate interest[1]—a legal basis that is widely adopted by EU firms under the GDPR. Moreover, the PIPL requires establishing a dedicated entity or appointing a representative inside China for international firms overseas, while the GDPR does not. On the other hand, the GDPR also has stricter rules than the PIPL. The firms processing data on behalf of others have to fulfil several obligations explicitly pointed out under the GDPR ('data processors'), which is not the case for the PIPL ('entrusted persons').

Effect of Legal Strictness on the Value for Actors in the Online Advertising Market

Actors Affected by Privacy Laws in the Online Advertising Market

There are three primary actors in the online advertising industry: (a) advertisers that aim to draw users' interest to the advertisers' offerings, (b) publishers (e.g.,

websites or apps) that monetize their services by selling ad spaces to advertisers and (c) users who are mainly interested in the publishers' offerings and sometimes interested in the ads displayed.

Figure 1 illustrates the three exchanges among the actors (Skiera et al., 2022):

- **Exchange 1:** Publishers provide users free content in exchange for processing users' data and providing contact between users and advertisers.
- **Exchange 2:** Advertisers pay publishers to contact users and pay more if receiving users' personal data help to improve the ad effectiveness.
- **Exchange 3:** Users may purchase the advertisers' offerings after seeing the ads targeted for the users.

Tracking and profiling play a vital role in each exchange because it enables advertisers to target users with ads and measure their ads' performance (e.g., click-through rate or conversion rate). Privacy laws provide users with rights and impose obligations on firms (e.g., advertisers or publishers) to restrict data processing (i.e., tracking and profiling). Therefore, we identify advertisers, publishers and users as the actors affected by privacy laws in the online advertising market and list them in the first column of Table 3.

Definition of Value for Actors

Following Kumar and Rajan (2007), we define value for an actor as the net accrued benefits (tangible and intangible) over the associated costs that firms and individuals realize in an exchange process. The creation and destruction of value happen alongside the exchanges in Figure 1.

Figure 1. Illustration of the Interactions Between the Relevant Actors of Privacy Laws in the Online Advertising Industry.

Source: Skiera et al. (2022).

Table 3. Detailed Effects of Legal Strictness on the Value for Publishers, Advertisers and Users.

Actors in the Online Advertising Market	Definition of Actors' Value and Sources of Variations of Value				Effects on Value Brought by Privacy Laws[a]	How Privacy Laws Affect the Value	Exemplary Measures of Value	Exemplary Studies
	Value	Creation/ Destruction	Exchange	Sources of Value Creation/Destruction				
Publishers	Profit = Revenue – cost	Revenue (creation)	1 (publisher ⇄ user)	User contacts and user data for tracking and profiling	Decreases/None (↓/→)	• Consent wall, users opting out, less web traffic, fewer data and less tracking • Heterogeneous for different sizes/categories	Page loads, user visits and third-party tracker existence	Congiu et al. (2022); Goldberg et al. (2021); Peukert et al. (2022); Schmitt et al. (2021)
			2 (publisher ⇄ advertiser)	Ad revenue = Price per ad × number of ads	Decreases (↓)	• Fewer personal data, lower WTP[b] and lower price per ad • Less web traffic and fewer ads to provide	Ad revenue, prices per ad and number of ad biddings	Johnson et al. (2020)
					Increases (↑)	• Increased market concentration and industry leader benefits (e.g., Facebook)		Kostov & Schechner (2019)
		Cost (destruction)	1 (publisher ⇄ user)	Cost of providing publisher offerings[c]	None (→)			
				Cost of getting user contacts and data	Increases (↓)	• Cost of managing consent and cost of understanding the laws, penalties	Price of CMP[d] services, TCF[e] registration fee and fine	Presthus & Sønslien (2021); NOYB (2021)
			2 (publisher ⇄ advertiser)	Cost of transferring user data	Increases (↓)	• Cost of ensuring advertisers have user consent		

(Table 3 continued)

(Table 3 continued)

Actors in the Online Advertising Market	Definition of Actors' Value and Sources of Variations of Value				Effects on Value Brought by Privacy Laws[a]	How Privacy Laws Affect the Value	Exemplary Measures of Value	Exemplary Studies
	Value	Creation/ Destruction	Exchange	Sources of Value Creation/Destruction				
Advertisers	Profit = Revenue – cost	Revenue (creation)	2 (publisher ⇄ advertiser)	User contacts and user data for tracking and profiling	Decreases (↓)	• Consent wall, users opting out, less web traffic, fewer data and less tracking • Publishers drop vendors to avoid legal risks	Page loads, reach to users and amount of tracking	Johnson et al. (2022); Sakamoto & Matsunaga (2019)
					Increases (↑)	• Increased market concentration and industry leader benefits (e.g., Google)		Greif (2018)
			3 (advertiser ⇄ user)	Revenue from advertiser offerings[f] = Price per offering × number of purchased offerings brought by targeted ad	Decreases (↓)	• No change in the price per offering • Less personal data, lower target accuracy and fewer purchased offering	Target accuracy and number of sales	Goldfarb & Tucker (2011); Zhao et al. (2021)
		Cost (destruction)	2 (publisher ⇄ advertiser)	Ad spending = Price per ad × number of ads	Decreases (↑)	• Fewer personal data, lower WTP and lower ad price • Less web traffic; fewer ad impressions	Ad revenue, ad prices and number of ad biddings	Johnson et al. (2020)
			3 (advertiser ⇄ user)	Cost of targeting users	Increases (↓)	• Cost of getting consent, cost of understanding the laws and penalties	Price of CMP services, TCF registration fee, and fine	Wolff & Atallah (2021); Kamps & Runte (2021)
Users	Net utility = Utility – disutility	Utility (creation)	1 (publisher ⇄ user)	Utility from publisher offerings	None (→)			
				Utility from personalized publisher offerings	Decreases/None (↓/→)	• Cost of opt-in for personalization • Heterogeneous for users with different preferences	Utility from personalization, and opt-in rate for personalizing purposes	Ichihashi (2020)

(Table 3 continued)

(Table 3 continued)

Actors in the Online Advertising Market	Definition of Actors' Value and Sources of Variations of Value				Effects on Value Brought by Privacy Laws[a]	How Privacy Laws Affect the Value	Exemplary Measures of Value	Exemplary Studies
	Value	Creation/ Destruction	Exchange	Sources of Value Creation/Destruction				
Users			3 (advertiser ⇄ user)	Utility from purchasing what they need (advertiser offerings)	None (→)			
				Utility from personalized ads	Decreases/None (↓/→)	• Cost of opt-in for personalization • Heterogeneous for users with different preferences	Utility from personalization, and opt-in rate for personalization purposes	Choi et al. (2021); Godinho de Matos & Adjerid (2021)
		Disutility (destruction)	1 and 3 (publisher ⇄ user) and (advertiser ⇄ user)	Disutility from the loss of privacy	Decreases (↑)	• Positive feeling from having control over their personal data • Heterogeneous for users with different preferences	Utility for privacy, and opt-out rate	Aridor et al. (2020); Johnson et al. (2020); Liu et al. (2022)
					Increases (↓)	• Cost of deciding on giving consent/opting out	Time spent making decisions	Skiera et al. (2022)

Source: The authors.

Notes: [a]In this column, the arrows (shown in brackets) represent the direction of changes in value (relative effects). For example, an increase in cost negatively affects the value, hence the cell has a down arrow even though it is an 'increase'. When finding a mixture of no effect and effects in one direction in the literature, we list both effects and conclude in one row. When finding a mixture of effects in opposite directions, we list them in two separate rows.
[b]WTP: Willingness to pay.
[c]Example of a publisher offerings: news and videos.
[d]CMP: Consent management platform.
[e]TCF: Transparency and consent framework.
[f]Examples of an advertiser offering: products and services.

Columns 2–5 of Table 3 specify the value for each actor and point out the sources of value creation and destruction within each exchange. For each actor (Column 1), we first define the value (Column 2), then categorize value change into creation and destruction (Column 3) and examine (Column 4) the sources of value creation and destruction in every exchange (Column 5). In economic studies, the fundamental assumption for a firm's objective is profit maximization (Mas-Colell et al., 1995). Given the assumption, we define the value for publishers and advertisers as profit, which is the difference between revenue and cost. Thus, gaining revenue represents value creation, and bearing cost denotes value destruction. Likewise, the value for users is the net utility, which equals (gross) utility minus disutility. Obtaining utility is a way to create value for users, while having disutility destroys user value.

From each actor's perspective, value creation and destruction happen simultaneously in every exchange. Take Exchange 1 as an example: publishers create value for users by providing (personalized) offerings (e.g., news and videos). At the same time, publishers destroy user value because the processing of personal data infringes user privacy. Users create value for publishers with their exposure and personal data while destroying publisher value due to the associated cost of creating the offerings and processing the data.

Effects of Privacy Laws on the Value for Actors

Detailed Effects of Privacy Laws on the Value for Actors

After defining value and outlining how value is created and destructed, we take a privacy law as a policy shock to the market and investigate its effects on value, with the counterfactual being no privacy law in force. The final four columns of Table 3 display the outcomes. We first point out the conclusion (Column 6) and explain the underlying mechanism (Column 7), then we propose a few exemplary measures of value (Column 8) and show the academic studies and industry reports that we base on (Column 9).

Methodology for the Investigation of Detailed Effects

This study primarily focuses on the direct effects[2] of privacy laws and discusses some of the indirect effects at the end of this section. Our conclusions come from a literature review on the effects of privacy laws on the online advertising market. We use the following data and procedure for our literature review:

1. **Literature database:** Web of Science Core Collection, Semantic Scholar, SSRN, industry reports and news articles.
2. **Filtering conditions:** Past five years (2018–2022), business and economics related, journal article/review/conference proceedings/books.
3. **Keywords:** General Data Protection Regulation, California Consumer Privacy Act, Personal Information Protection Law, privacy, privacy + *x* (*x* refers to a specific keyword in the sources of value creation/destruction in Column 5, e.g., 'ad revenue').

We then categorize findings from the sampled literature by actors, whether value creation or destruction, the exchanges involved, and sources of value creation and destruction. Next, the categorized findings fit in the appropriate row. We assume the conclusions hold for all general privacy laws. Note that the studies either examine the impact of the GDPR directly or discuss it in the context of general privacy laws because very few studies build on the CCPA and the PIPL.

Column 6 of Table 3 displays the absolute effects on value in words and shows the relative effects brought to the value (with arrows shown in brackets: up arrow for a positive effect, down arrow for a negative effect and right arrow for no effect). For example, an increase in cost negatively affects the value, hence having a down arrow even though it is an 'increase'. We take the average outcomes when finding heterogeneous effects among actors in the literature. When finding a mixture of no effect and effects in one direction, we list both effects and conclude in one row. When finding a mixture of effects in opposite directions (e.g., some studies find an increase, others find a decrease), we list them and conclude in two separate rows.

Results of the Investigation of the Detailed Effects

We observe that the effects of privacy laws on the value for actors are heterogeneous. On the firm side, the size and sometimes even the sign of the impact of privacy laws differ for different firms. Regarding the size of a firm, Congiu et al. (2022) find an inverted U-shaped relationship between publisher size and change in user contacts due to privacy laws, while other studies suggest that smaller firms suffer more losses (Campbell et al., 2015; Peukert et al., 2022; Sharma et al., 2021). Regarding the category of a firm, Schmitt et al. (2021) find negative effects on publishers' user contacts throughout the observation period for some industries (e.g., Arts and Entertainment) and positive effects for some others (e.g., Business and Consumer Services), whereas positive effects occur in the short term and negative effects in the long term for categories such as e-commerce and shopping.

On the user side, privacy laws have heterogeneous effects on users with different preferences for personalization. For those who used to be in favour of personalized offerings from publishers and advertisers (e.g., recommending content or products that may interest the user), utility from personalization decreases because privacy laws make personalization more costly with the opt-in consent banner (or the opt-out consent banner under the CCPA). Meanwhile, for those who do not obtain utility from personalization, the consent banners do not change their utility from personalized recommendation. Besides, privacy laws have heterogeneous effects on users with different sensitivity to privacy infringement. Users more sensitive to a privacy loss benefit more from the protection from privacy laws.

The indirect effects of privacy laws also impact the value change of actors. For instance, the ad revenue of publishers (respectively, the ad spending of advertisers) may stay unchanged. Since most ads whose value varies with the amount of personal data available are behavioural targeting ads, firms may strategically adjust their ad budgets toward contextual targeting ads, rendering an overall stable value from advertising. Another example is that user utility from consuming

publisher offerings may decrease; hence, value decreases. Due to reduced ad revenue, publishers cannot afford the cost of providing high-quality offerings. Therefore, the quality of publisher offerings drops.

Sum of Effects of Privacy Laws on the Value for Actors

To provide an overview of the effects aggregated by actors, we create a measure called the *sum of effects on value* and summarize the effects in Table 4. In Panel A, we assign a sum of '1' to the cells with up arrows, indicating a positive *sum of effects on value* ('0' to right-arrow cells, '−1' to down-arrow cells, '−0.5' to rows with down and right arrows). The final column of Table 4 Panel A aggregates the *sum of effects on value* by each actor, assuming (a) each row contributes equally (with equal weight) to the total outcome of the actor and (b) the effects within each row are homogeneous among actors. Panel B displays a summary of the *sum of effects on value*.

Table 4. Sum of Effects of Legal Strictness on the Value for Publishers, Advertisers and Users.

Panel A. Sum of Effects by Sources of Value Creation and Destruction.

Source ID	Actors	Sources of Value Creation and Destruction	Absolute Effects on Value Brought by Privacy Laws[a]	Sum of Effects on Value[b]	Total Sum of Effects on Value[c]
1	Publishers	User contacts and user data for tracking and profiling	Decreases/None (↓/→)	−0.5	−2.5
2		Ad revenue = Price per ad × Number of ads	Decreases (↓)	−1	
3			Increases (↑)	1	
4		Cost of providing publisher offerings[d]	None (→)	0	
5		Cost of getting user contacts and data	Increases (↓)	−1	
6		Cost of transferring user data	Increases (↓)	−1	
7	Advertisers	User contacts and user data for tracking and profiling	Decreases (↓)	−1	−1
8			Increases (↑)	1	
9		Revenue from advertiser offerings[e] = Price per offering × Number of purchased offerings brought by targeted ad	Decreases (↓)	−1	
10		Ad spending = Price per ad × Number of ads	Decreases (↑)	1	
11		Cost of targeting users	Increases (↓)	−1	

(Table 4 continued)

(Table 4 continued)

Source ID	Actors	Sources of Value Creation and Destruction	Absolute Effects on Value Brought by Privacy Laws[a]	Sum of Effects on Value[b]	Total Sum of Effects on Value[c]
12	Users	Utility from publisher offerings	None (→)	0	−1
13		Utility from personalized publisher offerings	Decreases/None (↓/→)	−0.5	
14		Utility from purchasing what they need (advertiser offerings)	None (→)	0	
15		Utility from personalized ads	Decreases/None (↓/→)	−0.5	
16		Disutility from the loss of privacy	Decreases (↑)	1	
17			Increases (↓)	−1	

Source: The authors.

Notes: [a]In this column, the arrows (shown in brackets) represent the direction of changes in value (relative effects). When finding a mixture of no effect and effects in one direction in the literature, we list both effects and conclude in one row. When finding a mixture of effects in opposite directions, we list them and conclude in two separate rows.
[b]We assign '1' to the sum of effects on value where the row contains an up arrow, indicating a positive sum of effects on value ('0' to rows with right arrows, '−1' to rows with down arrows, '−0.5' to rows with down and right arrows).
[c]We add up the sum of effects on value for each actor, assuming each row contributes equally (with equal weight) to the total sum of effects on value.
[d]Example of a publisher offering: news, videos.
[e]Example of an advertiser offering: products, services.

Panel B: Summary of Sum of Effects on Value.

	Sum of Effects on Value			
Actors	Negative	Positive	None	Total
Publishers	−3.5	1	1.5	−2.5
Advertisers	−3	2	0	−1
Users	−2	1	3	−1
Total	−8.5	4	4.5	−4.5

Source: The authors.

Note: A negative value of the sum of effects on value indicates a decrease in the value for each actor (down arrow), while a positive value of the sum of effects on value indicates an increase (up arrow).

We conclude that the overall effects of privacy laws on value are most negative for publishers (*sum of effects on value* = −2.5; 3.5/6 negative, 1/6 positive and 1.5/6 none) and is similar for advertisers (*sum of effects on value* = −1; 3/5 negative and 2/5 positive) and users (*sum of effects on value* = −1; 2/6 negative, 1/6 positive and 3/6 none).

According to the literature review, we summarize that the negative effects of privacy laws come from three sources: (a) users or the consent management tools (e.g., a browser extension) making choices to opt-out from data processing, (b)

firms making choices to work with fewer firms to avoid legal risks and (c) legal requirements imposing compliance cost to users and firms. As a result of (a) and (b), fewer user contacts and user data for tracking and profiling are available. Fewer personal data lower firms' targeting accuracy, decreasing publisher ad revenue and advertisers' revenue from their offerings. Because of (c), firms bear the cost of creating technical and legal infrastructures, as well as the risk of violating the laws. Users have the decision cost to take control of their data, both opt-in and opt-out.

The positive impact of privacy laws mainly originates from three sources: (a) users gaining utility from privacy protection; (b) industry leaders such as Facebook and Google benefiting from the increased market concentration—a larger share of a smaller pie; and (c) zero-sum value transfer from advertisers to publishers—the decrease of publisher ad revenue equals the decrease of advertiser ad spending, that is, lower cost and higher value for advertisers.

Comparison of the Effects of the Three Privacy Laws on Value

Results of the Comparison of the Effects of the Three Privacy Laws on Value

Table 5 quantifies the changes in value brought by each privacy law for each actor. The measure *changes in value* is the product of (a) the *legal strictness score* (developed in the section titled Comparison of the Three Privacy Laws) and (b) the *sum of effects on value* (introduced in the section titled Effects of Privacy Laws on the Value for Actors). With *changes in value*, this study compares the changes in value across each privacy law and each actor.

Table 5. Summary of Effects of the Three Privacy Laws (GDPR, CCPA, PIPL) on the Value for Publishers, Advertisers and Users.

	Changes in Value			
Actors	GDPR (18)	CCPA (5)	PIPL (16)	Total
Publishers (−2.5)	−45	−12.5	−40	−97.5
Advertisers (−1)	−18	−5	−16	−39
Users (−1)	−18	−5	−16	−39
Total	−81	−22.5	−72	

Source: The authors.

Note: Numbers in the brackets are the total legal strictness score for each privacy law (Row 2) or the total sum of effects on value for each actor (Column 1). We fill each cell with changes in value (product of legal strictness score and sum of effects on value) brought by each privacy law for each actor in the online advertising market.

First, stricter privacy laws bring larger negative changes to the value for actors. Specifically, the GDPR brings the largest negative changes to value (−81),[3] followed by the PIPL (−72) and the CCPA (−22.5), which holds for the whole market and all actors. Many academic studies find that regulatory strictness correlates with various economic outcomes such as decreased page views and revenue (Goldberg et al., 2021), decreased publisher-vendor connections (Johnson et al., 2022) and decreased venture investment (Jia et al., 2021), and, thus, support this conclusion.

We provide some examples to explain the conclusion. Recall the criteria for comparing the contents of privacy laws we adopt in concluding strictness in the section titled Methodology for the Comparison of the Three Privacy Laws. Take penalties as an example. Privacy laws with penalties of a smaller scale are less strict. Therefore, the CCPA (*legal strictness score* in penalty = 0) is less strict than the GDPR and the PIPL (for both, *legal strictness score* in penalty = 2) in terms of penalty. The changes in the value for actors brought by the CCPA are smaller than the other two laws. As Johnson et al. (2022) point out, publishers with larger potential penalties cut off more connections with technology vendors.

Second, the changes in value are the largest in absolute terms for publishers, followed by users and advertisers. The final column of Table 5 supports the conclusion with publishers having a change of −97.5, advertisers a change of −39 and users a change of −39. The finding holds for all privacy laws, as we observe in each column of Table 5.

Limitation of Comparison

To provide quantitative evidence for the conclusions, we develop a method with three measures: the *legal strictness score*, the *sum of effects on value* and the *changes in value*. The assumptions this study imposes on the measures generate limitations. Take the *legal strictness score* as an example. First, the rule of scoring legal strictness built upon the rankings and, thus, neglects the size of the differences. A time difference (enforcement) of three years, two year and one year has an identical score with a time difference of nine years, five years and one year. Second, calculating the total score for each privacy law by adding up assumes an equal weight of each criterion. However, some criteria may contribute less to the overall strictness, such as the enforcement time. Therefore, we primarily interpret the ranks of the measures and not the absolute values.

Conclusion and Implication

This article discusses the different changes in the value for actors in the online advertising market (publishers, advertisers and users) brought by three different privacy laws (GDPR, CCPA and PIPL). Our study concludes that stricter privacy laws bring larger negative changes to the value for actors. The changes in value are the largest in absolute terms for publishers, followed by users and advertisers.

Besides, the overall effects of privacy laws on value are negative, which holds for the whole market and each actor. The effects can be heterogenous for the actors though.

The overview of differential effects of privacy laws on the value for various actors provides more information for regulators who have to balance the value for all actors when introducing new privacy laws or amendments. Firms, especially international firms, gain more insight into how to create value for users and how others create value for them under different privacy laws. We also offer a method for academics and practitioners to systematically compare differential effects under various regulations.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No. 833714).

Notes

1. Applicable to a situation where personal data processing is 'necessary for the legitimate interest pursued by a data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the [user]' (Art. 6 point (1f), GDPR).
2. Direct effects of privacy laws: the actors only take one action to generate the effect (e.g., ad revenue decreases: publishers provide fewer ads). Indirect effects of privacy laws: the actors take more than one action to generate the effect (e.g., user utility from consuming publisher offerings decreases: publishers provide fewer ads, ad revenue decreases and publishers only afford to provide offerings with lower quality).
3. The numbers in the brackets are the total changes of value for the whole online advertising market (publishers, advertisers and users combined).

References

Aridor, G., Che, Y.-K., Nelson, W., & Salz, T. (2020). *The economic consequences of data privacy regulation: Empirical evidence from GDPR* (SSRN Scholarly Paper ID 3522845). Social Science Research Network. https://doi.org/10.2139/ssrn.3522845

Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy regulation and market structure: Privacy regulation and market structure. *Journal of Economics & Management Strategy, 24*(1), 47–73.

Carmagnola, F. (2008). The five Ws in user model interoperability. In *Ubiquitous user modelling* (pp. 20–36). D. Heckmann et al.

Choi, W. J., Jerath, K., & Sarvary, M. (2021). *Consumer purchase journey, targeted advertising, and privacy choices* (Working Paper). Summer Institute in Competitive Strategy (SICS), Haas School of Business. https://sics.haas.berkeley.edu/Programsics2021.html

Congiu, R., Sabatino, L., & Sapi, G. (2022). *The impact of privacy regulation on web traffic: Evidence from the GDPR* (SSRN Scholarly Paper ID 4025033). Social Science Research Network. https://doi.org/10.2139/ssrn.4025033

Godinho de Matos, M., & Adjerid, I. (2021). Consumer consent and firm targeting after GDPR: The case of a large telecom provider. *Management Science*, *68*(5). https://doi.org/10.1287/mnsc.2021.4054

Goldberg, S., Johnson, G., & Shriver, S. (2021). *Regulating privacy online: An economic evaluation of the GDPR* (SSRN Scholarly Paper ID 3421731). Social Science Research Network. https://doi.org/10.2139/ssrn.3421731

Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management Science*, *57*(1), 57–71. https://doi.org/10.1287/mnsc.1100.1246

Greif, B. (2018, 10 October). Study: Google is the biggest beneficiary of the GDPR. *Cliqz*.

Ichihashi, S. (2020). Online privacy and information disclosure by consumers. *American Economic Review*, *110*(2), 569–595. https://doi.org/10.1257/aer.20181052

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review, 10*(1), 18–26.

Jehl, L., & Friel, A. (2018). *CCPA and GDPR comparison chart*. https://www.bakerlaw.com/articles/alan-friel-laura-jehl-create-chart-comparing-ccpa-and-gdpr

Jia, J., Jin, G. Z., & Wagman, L. (2021). The short-run effects of the general data protection regulation on technology venture investment. *Marketing Science*, *40*(4), 661–684. https://doi.org/10.1287/mksc.2020.1271

Johnson, G. A., Shriver, S. K., & Du, S. (2020). Consumer privacy choice in online advertising: Who opts out and at what cost to industry? *Marketing Science*, *39*(1), 33–51. https://doi.org/10.1287/mksc.2019.1198

Johnson, G., Shriver, S., & Goldberg, S. (2022). Privacy & market concentration: intended & unintended consequences of the GDPR. *Social Science Research Network.* https://doi.org/10.2139/ssrn.3477686

Kamps, M., & Runte, C. (2021). *GDPR enforcement tracker report—2nd edition 2021*. https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report

Kostov, N., & Schechner, S. (2019, 31 May). Google emerges as early winner from Europe's new data privacy law. *Wall Street Journals*.

Kulbeth, M. (2021). *A deep dive into China's new privacy law*. https://www.sixfifty.com/blog/a-deep-dive-into-chinas-new-privacy-law/

Kumar, V., & Rajan, B. (2017). What's in it for me? The creation and destruction of value for firms from stakeholders. *Journal of Creating Value*, *3*(2), 142–156. https://doi.org/10.1177/2394964317723449

Kumar, V. & Reinartz, W. (2016). Creating and enduring customer value. *Journal of Marketing, 80*(6), 36–68.

Liu, J. Z., Sockin, M., & Xiong, W. (2022). *Data privacy and temptation* (SSRN Scholarly Paper ID 3670488). Social Science Research Network. https://papers.ssrn.com/abstract=3670488

Mas-Colell, A., Whinston, M. D., & Green, J. R. (1995). *Microeconomic theory* (Vol. 1). Oxford University Press.

Marini, A., Kateifides, A., Bates, J., Zanfir-Fortuna, G., Bae, M., Gray, S., & Sen, G. (2018). *Comparing privacy laws: GDPR v. CCPA*. https://fpf.org/blog/comparing-privacy-laws-gdpr-v-ccpa/

Noyb. (2020). *Noyb files 422 formal GDPR complaints on nerve-wrecking 'cookie banners'*. https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners

Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T. (2022). Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Science*, *41*(4). https://doi.org/10.1287/mksc.2021.1339

Presthus, W., & Sønslien, K. F. (2021). An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems and Project Management*, *9*(1), 38–53. https://doi.org/10.12821/ijispm090102

Sakamoto, T., & Matsunaga, M. (2019). After GDPR, still tracking or not? Understanding opt-out states for online behavioral advertising. In *2019 IEEE Security and Privacy Workshops (SPW)* (pp. 92–99). IEEE. https://doi.org/10.1109/SPW.2019.00027

Schmitt, J., Miller, K. M., & Skiera, B. (2021). *The impact of privacy laws on online user behavior* (SSRN Scholarly Paper ID 3774110). Social Science Research Network. https://doi.org/10.2139/ssrn.3774110

Sharma, P., Sun, Y., & Wagman, L. (2021). The differential effects of privacy protections and digital ad taxes on publisher and advertiser profitability. *Social Science Research Network.* https://doi.org/10.2139/ssrn.3503065

Skiera, B., Miller, K., Jin, Y., Kraft, L., Laub, R., & Schmitt, J. (2022). *The impact of the general data protection regulation (gdpr) on the online advertising market*. Self-Publishing.

Wolff, J., & Atallah, N. (2021). Early GDPR penalties: Analysis of implementation and fines through May 2020. *Journal of Information Policy*, *11*(1), 63–103. https://doi.org/10.5325/jinfopoli.11.2021.0063

Zhao, Y., Yildirim, P., & Chintagunta, P. K. (2021). *Privacy regulations and online search friction: Evidence from GDPR* (SSRN Scholarly Paper ID 3903599). Social Science Research Network. https://doi.org/10.2139/ssrn.3903599