Eastern Journal of European Studies
DOI: 10.47743/ejes-2024-0208 ● December 2024 ● VOLUME 15, ISSUE 2

Data, digital markets, and the economic value of privacy

Luca Zamparini ✉
University of Salento, Lecce, Italy

Abstract
The paper considers the role that the development of digital markets has played on the economic value of privacy in the last decades. It first discusses the possible definitions of privacy by highlighting the high degree of heterogeneity. It then assesses the economic value of privacy and how it has been influenced by digital technologies, in terms of costs, benefits and externalities. The paper also examines the digital paradox, i.e. the dichotomy between privacy attitudes and privacy behavior. It then proposes a series of empirical findings on the value of digital privacy, by underscoring the high degree of contextuality of this measure. Lastly, the paper discusses the relevance of regulations, especially the General Data Protection Regulation by the EU and the California Privacy Rights Act, to meet the requirements of fair information practices and their economic effects.

Keywords: data, digital markets, economic value of privacy, theoretical and empirical findings, public regulations

Introduction

The last decades have witnessed the widespread diffusion of digital technologies and markets. Such phenomena have had a deep impact on how people live, work, and interact with each other (Anisimov & Ryzhenkov, 2021; Gokmenoglu & Kaakeh, 2022; Kourtit, 2019). An element of the individuals that has been momentously influenced is definitely privacy. This concept has extended its traditional real-life realm to encompass its digital dimension. This has also implied the necessity to elaborate its definition by considering these developments. Digital privacy and the related communication of sensitive personal data have modified the protocols, strategies and activities of firms operating in virtually all markets, with important economic effects. On the one hand, firms have proposed new products and services. Moreover, they have also been innovating their business models. In this context, the traditional consideration that the lack of perfect information poses problems to the efficient and effective functioning of markets has been complemented by the economic value that privacy may have for individuals. Moreover, the protection of privacy must take into consideration the technological innovations and the

✉ Associate Professor, Department of Law Studies, Economics Division, University of Salento, Lecce, Italy; e-mail: luca.zamparini@unisalento.it.

consequent increase in the possibility of breaching such protection. It may also be the case that consumers should be compensated for the disclosure of personal, sensitive data. The management of massive amounts of such data, whose costs of acquisition appear to have lowered over time due to the diffusion of machine learning and of other data processing technologies, has also generated the diffusion of dedicated firms and markets. Consequently, digital privacy has been carefully taken into account by public administrations and scholars alike. A clear definition of digital privacy and an assessment of the economic effects of their uses are important requirements to develop and foster fair data and privacy management and to maximize the social welfare, by trying to minimize the costs and negative externalities and to maximize the benefits and positive externalities.

The paper aims to introduce and discuss the main theoretical and empirical findings emerging from a review of the relevant literature. Moreover, it will consider the public regulations that have been issued, mainly the General Data Protection Regulation of the EU and the California Privacy Rights Act, by particularly presenting the findings in terms of economic effects of such regulations. It is structured as follows. The first section considers the possible definitions of privacy that have been proposed over time and how this definition has been contextualized in digital environments. The second section proposes a review of the theoretical framework of the economic value of privacy and digital technologies, and it also discusses the digital paradox, or the difference between privacy behaviour and attitudes. The third section analyses a series of empirical findings on the value of digital privacy. The fourth one underlines the relevance of regulations and their economic effects. The last section concludes.

1. Definitions of privacy

According to Lukacs (2016), the definition of privacy has undergone a long evolution over time, and it is definitely contextual to historical periods, societies and individuals. Consequently, it is quite unlikely that any definition of privacy may ever be considered as universal and conclusive. The first instance of the modern notion of the term appears to have been proposed by Brandeis and Warren in 1890 as “the right to be left alone”. Quite interestingly, these authors already mentioned technological development (in their study they referred to photographs) and gossip as possible sources of breaches of privacy. This basic concept has been elaborated over time. A good summary of all proposed definitions can be related to the six categories, proposed by Solove (2011), to which privacy may refer to: a) control of personal information; b) intimacy; c) limited access to the self; d) personhood; e) right to be left alone; and f) secrecy. The first category considers the freedom of an individual to decide which information about herself or himself can be made public and which others have to be kept classified. A similar line of reasoning is related to the second category that only elicits the information that constitute the intimacy, and consequently, the private dominion of a person. The third one involves the concealment or withholding of private information. The personhood approach refers to the autonomy of all the details connected to personal identity, complemented by the fifth and the sixth categories concerning the right to be left alone and to have some parts of information covered by secrecy.

Another survey proposed by Moore (2008) has recognized the high degree of heterogeneity of possible definitions of privacy and it has tried to divide them according to three different classifications. The first one takes into consideration descriptive and normative accounts of privacy. The descriptive accounts are related to factual states or conditions. The normative ones imply moral claims or obligations, such as ethical considerations. Another relevant partition is connected to the reductionist and non-reductionist accounts. The first ones argue that privacy is not an original right, but it rather derives from other rights, such as liberty, property or life. The consideration of privacy is then justified when other, primary, rights have to be protected. On the contrary, the non-reductionist approach safeguards privacy as a distinct, relevant, right from other moral concepts or values. Lastly, Moore (2008) distinguishes between control-based and use-based definitions of privacy. They refer to the access control right over the information about oneself. This can have either a positive (the actual management of information) or a normative (focusing on moral and ethical claims) treatment.

By taking into consideration all the possible definitions of privacy and their degree of heterogeneity, part of the research has pondered privacy in an economic context. The paper by Posner (1981) can be considered as one of the seminal, theoretical works. The author states that privacy and information are tightly connected to each other. In this context, the concealment of information can hamper the allocative efficiency of markets, as in the case of employers and employees' relationships or in the case of the credit markets. The author concludes that privacy should be guaranteed by law only when it refers to intimate information about individuals and their right to keep them concealed.

VanAaken et al. (2014) have surveyed the relationships between privacy, freedom, and economics. They have stated that technological advances (mainly connected to the Internet) have made the reduction of privacy ever higher. In some cases, this may be in favour of the person whose privacy is reduced, as in the cases of medical treatments which need to be based on the larger possible knowledge about the patient's conditions. Moreover, coherently with the literature related to adverse selection, the concealment of information may be detrimental in several markets, such as employment, placement, and insurance. In more general terms, VanAaken et al. (2014) claim that part of the literature has tried to identify the right amount of privacy. This should be determined in conjunction with other important values (e.g. security and wealth). The authors then claim that privacy should be considered as a particular form of freedom. Consequently, it has in itself an intrinsic value that should be determined regardless of any other theme. This implies that any individual can trade elements of her/his own privacy as long as the consent is voluntary and informed, as for any other traded good. However, in actual circumstances, it is often the case that individuals do not fully evaluate the consequences of providing some personal information or allowing its retrieval or acquisition. VanAaken et al. (2014) then consider that individuals should be allowed a two-level control in the context of privacy. The first level would be represented by the agreement of the individual. The second level would be constituted by the possibility to exert an exit option, once the consequences of one's agreement to the reduction of privacy become evident. While the first level may be skipped, the second one should never be given up or traded.

De Capitani di Vimercati et al. (2012) have contextualized the privacy issues in the case of data that could be retrieved by questionnaires or via the web. They introduce the distinction between syntactic privacy, that entails the possibility of diffusing data only when they are related to a certain number of individuals in the population or in the sampled group, and semantic privacy, which considers the release of data only when these have been perturbed by adding noise to the original ones. The syntactic approaches to data and privacy protection are related to the anonymity of them and of their attributes. Such approaches, coherently with the literature that has been previously considered in this section, may take into account the personal privacy preferences of single individuals or of categories of people. The semantic approaches consider differential privacy as the possibility to release microdata only when they do not allow to disclose sensitive information about any individual. Such concept may be limited in the cases in which part of the information is of higher interest. Such distinctions are particularly relevant in the cases in which digital technologies are considered, as will be discussed in the next section.

2. Economic value of privacy and digital technologies

Acquisti et al. (2016) have proposed a thorough review of the various lines of economic research that have tried to define the value of privacy and of personal data in the context of digital technologies' development. They have considered three waves of research. The first one, spanning between the 1970s and 19080s, proposed a general economic discussion about the benefits or costs that individuals, markets, or societies may be exposed to, in cases in which personal information is not diffused. The second wave began in the mid-1990s when it became evident that the new digital information technologies determined novel economic themes pertaining to data retaining or sharing. This wave was similar to the first one in terms of methodology but differed with respect to the considered scenarios (e.g. cryptography and markets of personal data). The third wave, originating in the early 2000s, follows the same lines of research as the second one but proposes empirical analyses and more formal economic models. This was also due to the fact that the advent of Internet and of social networks have allowed to gather vast amounts of data, related to individual's attributes and traits (such as age, gender, income, preferences, and in some cases reservation prices) that have a momentous economic value. Such information can be traded with peculiar firms whose mission is to make profit out of them or, alternatively, to propose specific services, offers, and advertising. From an economic perspective, it has emerged that privacy is the control over data sharing. This determines a series of trade-offs both for the data holder and for the market as a whole. It may be that sharing personal data allows to obtain specific benefits, such as discounts, personalized services, reduced search costs, and higher accuracy of data retrieval. Moreover, positive externalities may emerge in the markets, as efficacy of pharmaceuticals, early alerts of epidemics, more efficient choices when there is the possibility to take advantage of other people’s assessments of specific goods and services. Choi et al. (2019) have proposed a theoretical model considering privacy and personal data collection when information externalities are present. They argue that the excessive collection of personal data leads to a monopoly market equilibrium that generates a degree of privacy that is inferior to the socially optimal one. This is mainly due to the users’ coordination failure and to the information externalities characterized by the possibility of data holders to infer relevant information about third parties, who may be similar to the data sharing individuals according to specific traits and characteristics. The authors also assert that a data market may emerge, even when data holders make up a fragmented market. The possibility of such forms of market for data is also investigated by Jones and Tonetti (2020) who assess that data is a nonrival good. As such, it may imply increasing returns and justify its broad use across firms because of social gains in the first periods of these markets. Subsequently, the returns to scale may drive the evolution towards a monopoly situation also because the availability of data may constitute a barrier to entry in the market. The authors also argue about the possibility of data being the result of an active investment strategy of the firms. Their nonrival nature may imply suboptimal levels of investment. The last part of the analysis by Jones and Tonetti (2020) is normative and discusses the possibility to give property rights about data to consumers versus the public regulations. The authors conclude that the first option may lead to better equilibria, as long as transaction costs and other market inefficiencies are overcome.

Acquisti et al. (2016) have argued that privacy may in some cases be considered as a final good, that has a value in itself, while in others it may stand as an intermediate one that allows to reach specific goals (as in the aforementioned case of the choice among different alternatives when assessments about them are present). A paper by Tesary (2022) has proposed a similar distinction by mentioning the intrinsic preferences (or *utility primitives)* and the instrumental ones; that are endogenously determined by the manner in which this private information can be used to modify the outcome of a transaction by the other involved party. A last theme that is mentioned (and that will be developed extensively in Section 3 of this paper) is the ambiguity of evaluating privacy given that either the willingness to accept money to disclose personal information or the willingness to pay to retain it may alternatively be considered. This issue has also been investigated by D'Annunzio and Menichelli (2022) in the context of the market for digital privacy. They have compared the availability of consumers to share personal data in order to obtain a discount versus their possibility to pay to retain these data. The authors determine that an important role is played by the manner in which the valuation of privacy is assessed. Important parameters are represented by the nature of the data that have to be shared. If consumers perceive that these data are easily accessed in other ways, they will be eager to trade them. On the contrary, they will be very reluctant to diffuse data about characteristics and traits that are more confidential and harder to associate with them. In the latter case, individuals may also be willing to pay firms or institutions that have them available in order to keep them classified. The relationships between the economic value of customers' information and privacy have also been investigated by Baumann et al. (2019) in the context of clickstream data and their potential to understand and predict consumers' behaviour in e-commerce. The authors consider how these data can determine behavioural traits of individuals and, consequently, pose threats to their privacy. The authors then perform an economic analysis that leads them to conclude that the gains for firms in terms of predictive accuracy are mostly related to the short term while storing the data over longer time horizons has a much lower value. Bansal et al. (2016) have proposed a complementary approach that describes how trust and privacy concerns are important in disclosing private information online. The critical factors that determine the degree of trust of individuals are grouped by the authors into two subsets. The first one refers to the context (e.g. individual attributes, location, prior positive experience with the website, prior perceived financial/health/personal information privacy invasion) within which consumers have to declare personal data and the second one deals with the customer's personality traits (i.e. agreeableness, conscientiousness, emotional instability, extroversion, and intellect). Both sets of elements are important given that certain data may involve vulnerabilities to social embarrassment, psychological violation of the private dimension, or monetary losses.

Goldfarb and Que (2023) have proposed a comprehensive analysis of the benefits that privacy and data flows provide to consumers and to firms and of the positive and negative externalities that originate from the availability of data. According to them, the main benefit of privacy for consumers is the possibility to avoid price discrimination practices carried out by firms on the basis of previous information. Another benefit may be constituted by the lack of targeted advertising that may not be accurately defined on the basis of poor targeting. When data flows are considered, better service, personalization and increased surplus appear as the main benefits. Examples of improvement of service and personalization are related to several different markets, as online commerce, and healthcare. In competitive markets, the disclosure of information about customers may enhance the competition among firms leading to lower prices, and higher surpluses, for consumers. Another example of the value of information for the demand side of the market is related to the usage-based car insurance, where safe drivers self-select themselves on the basis of their recorded behaviour to be granted lower risk premia. When firms are considered, the benefits of data flows are personalized pricing, targeted advertising, and customer relationship management. Moreover, data flows may determine the creation of specific firms, data intermediaries, who collect, aggregate and organize data. Such data are then sold directly to other firms or indirectly through sponsored search and retargeting. On the other hand, the benefits of privacy to firms are the reduction of costs of storage and security of the data from cyberattacks and the market power, as part of the literature has shown that a larger amount of data may increase price competition among firms and decrease quality based supply. Finally, Goldfarb and Que (2023) discuss the negative and positive externalities of data. The former are represented by the information about third individuals that originates from a person’s social media profile and interactions, by the consequent probabilistic correlations of preferences and behaviours, and by instrumental value of the data. The positive externalities refer to productivity and data economy and to socially beneficial behaviour.

2.1. The digital privacy paradox

Since the beginning of the third wave of economic analysis of the value of privacy and of personal data, various scholars have hypothesized the presence of a digital privacy paradox from both an analytical and an empirical viewpoint (Gerber et al., 2018; Kokolakis, 2017). Such paradox is related to the dichotomy between privacy behaviour and privacy attitude. This dichotomy has arisen through surveys that have indicated that individuals are willing to trade their personal data for small compensations while declaring that they are highly concerned about the possibility that such data may be collected, stored and used by private firms or by public administrations. The review by Kokolakis (2017) has concluded that the privacy paradox can be interpreted according to five different research themes: a) privacy calculus theory; b) social theory; c) cognitive biases and heuristics in decision making; d) decision making under bounded rationality and information asymmetry; and e) quantum theory homomorphism. According to the first research theme, people make a calculus that considers the potential gain of disclosure and the expected loss of privacy. If the former exceeds the latter, then the individual is eager to make some of the personal data public. Although the behaviour seems not coherent given these premises, this may be reasonable once intangible gains are computed. Social theory considers that the lack of a formalized representation of online privacy determines that individuals are not able to develop a reliable perspective on it and, consequently, they cannot clearly quantify its value. Cognitive biases may refer to affect, fuzzy boundaries and benefit heuristics, hyperbolic discounting, optimism, and overconfidence. Bounded rationality and information asymmetries are in line with general economic theory and imply that individuals are normally limited in terms of computational capacity and/or knowledge. In this context, the information asymmetries are related to the lack of knowledge about the uses of one's personal data by people who have mobile applications or belong to social networks. Lastly, the quantum theory homomorphism takes into account indeterminacy as the possibility that individuals may change their preferences. Gerber et al. (2018) have widened the possible causes leading to the privacy paradox by contemplating: a) the lack of personal experience and protection knowledge; b) social influence; c) the risk and trust model; and d) the illusion of control. The lack of experience is related to the fact that only a limited number of users have undergone a privacy invasion and its consequences (Martin, 2020). It is then difficult for all the others to correctly quantify the value of their online privacy. Social influence refers to the herding behaviour of people who wish to align their situation to those of their groups of friends or families. In the context of digital markets, this generates reciprocity and behaviours that differ from the stated attitude about data disclosures. The risk and trust model considers that individuals may be motivated by trust in their actual behaviour while perceived risk dominates the general attitude. Trust, as an environmental factor, generally prevails over risk in concrete situations. The illusion of control describes the situation in which users perceive that they are managing the publication of sensitive information. However, they do not realize that those data may be used afterwards for reasons and aims that are not evident to them. Gerber et al. (2018) finally ponder the possibility that the digital privacy paradox may be the result of the specific methodology that is used to test this hypothesis. Possible examples include the inappropriate operationalization or the multidimensional nature of privacy.

3. Empirical findings on the economic value of digital privacy

In the last decades, several papers have taken into account the theoretical discussions and findings that were analysed in Section 2, and they have proposed empirical evaluations of the economic value of privacy. One of the first studies is definitely the one carried out by Poindexter et al. (2006). The authors consider a sample of undergraduate and postgraduate university students who were exposed to the possibility of using different strategies to look for a job. Among the strategies, there would be a negative correlation between the payoff obtained in terms of salary and the possibility to keep the privacy of personal data. The main results of the study were the following two: a) individuals would be willing to shift to higher risky options once they perceived that policy actions were undertaken or that they would have the possibility to purchase protection against theft of personal data (with values exceeding $100); b) Internet users would be eager to pay important amounts of money to protect their privacy, especially when they perceive that the environment has become riskier.

In 2015, Savage and Waldman discussed the privacy trade-offs in smartphone applications. By using a US sample and a stated preferences exercise, they estimated that the representative consumer is eager to make some payments in order to conceal specific data; $1.19 for their location, $1.75 for their mobile phone's identification number, $2.28 for browser's history, $3.58 for their texts, and $4.05 for their contacts. Moreover, by considering some demographic characteristics of the respondents, they highlight that the willingness to pay increases with age, when the gender is female, and with higher degrees of education and of yearly income.

Hirschprung et al. (2016) have in turn referred to prospect theory (that relates the probability of privacy violation to the perceived cost) to estimate how individuals evaluate their privacy in information disclosure scenarios. Their methodology is based on a value of privacy estimator that presumes an iterative process in which people may accept or refuse a transaction that is also constituted by an information disclosure component. They apply this methodology to electronic commerce transactions. Their results show that the higher the probability of disclosure of information, the higher the compensation that individuals are requiring to make personal data public. Moreover, the value is connected to the sensitivity of the bought object (the highest value is by far related to the purchase of an adult toy ($35 for a probability of 0.3, $56.9 for a probability of 0.6), followed by smartphone ($16.4 and $21.7), notebook ($16.2 and $19)), asthma inhaler ($9 and $15.9), political book ($5.8 and $6.6), and rechargeable batteries ($2.8 and $3.9). A similar study has been carried out by Wang et al. (2016) who have considered the intention to disclose personal information via mobile applications. The authors stress that personalized services and self-presentation influence individuals' perceived benefits in a positive way. On the other hand, perceived control and severity are correlated to risk and lower the intention to disclose personal information. The authors also argue that as individuals become more aware of privacy protection or less concerned about it, they tend to consider trade-off values more closely. The market for digital privacy has also been investigated by D'Annunzio and Menichelli (2022) who have considered a Norwegian survey to analyse the difference between accepting to share personal data for a discount on the purchase of a good and the willingness to pay to keep those data concealed. Their main results affirm that the former is higher than the second for low sensitivity data. On the other hand, the latter is higher for data that personally identify the respondent. When the demographic characteristics and the attitudes of the respondents are considered, interesting considerations can be made both on the willingness to accept a discount and on the willingness to pay. The willingness to accept is particularly influenced by the personalization of services to the specific preferences and needs of the individuals and by the trust in the firms and institutions that provide internet services. According to this study, gender, personalization, and privacy concerns are not statistically significant determinants, while age and trust have negative effects. However, trust displays a positive effect when banks, financial institutions, mobile operators, and public administrations are considered. A similar experiment had been conducted by Winegar and Sunstein (2019) who have used a stated preference survey to estimate the value of data privacy among a sample of more than 2,400 US citizens. Their study concludes that the willingness to pay to retain personal data is much smaller than the willingness to accept compensation in order to make sensible data public. In this context, the willingness to accept strongly depends on the specific description of personal data. Physical and mental health appear as the categories to which individuals are more sensitive (requiring on average about $100 per month) while religion and sexual orientation are the less sensitive ones ($50 per month). The large difference between the willingness to pay and the willingness to accept is explained by the authors by using the concept of "super-endowment effect", that is the attribution of a much greater value to the things that people own with respect to those that they do not have. Skatova et al. (2023) have performed an experiment to test the willingness to pay to protect one's data by using a variety of data sharing environments in the United Kingdom. A first result of the study, in line with previous research, is that the willingness to pay depends on the peculiar personal data to conceal (on average more than £20 for bank transactions and medical records, more than £10 for mobile phone GPS data, browsing history and social media interactions, between £10 and £5 for electricity use, loyalty cards, and physical activity). Such values are higher than those obtained in previous works. Two other results that are contrary to previous research is that the willingness to pay decreases with age and that women show smaller values. On the other hand, higher education levels lead to higher willingness to pay, in line with previous research. Tesary (2022) considers a sample of 2,283 US citizens and concludes that the willingness to accept to share data is highly heterogeneous. The author also proposes some average values about a series of personal data where children, income, and intent rank highest while age and gender rank lowest.

To the best of the author's knowledge, the only survey of the value of online privacy across countries by date has been proposed by Prince and Wallsten (2022). The authors consider six countries (Argentina, Brazil, Colombia, Germany, Mexico, and United States) and 10 personal data items on different themes (biometrics, finances, location, networks, and web browsing). The economic measure used to quantify the value of privacy is the willingness to accept in order to share data. When the overall sample is considered, the following values of willingness to accept per month emerge: 1) financial balance ($8.44), 2) fingerprint ($7.56), 3) read texts ($6.05), 4) cash withdrawals ($5.80), 5) contacts ($4.92), 6) browsing history ($3.75), 7) voiceprint ($3.56), 8) info about own's network ($2.63), 9) location (1.82), 10) send ads ($-0.07). By considering the single countries' samples, Germany ranks first in terms of overall privacy valuation, followed by the United States and then the Latin American countries. By considering the demographic characteristics of surveyed people, it appears that female and older respondents attach a higher value of privacy to all considered items. When the level of income is taken into account, the results are mixed. Higher income individuals attach higher valuations to share balance, cash withdrawals, and info about their networks, and to read texts. On the contrary, lower income respondents display higher average estimates for fingerprints, contacts, browsing history, and voice print, and send ads. Such heterogeneities appear to be clearly connected to types of considered items.

4. The relevance of regulations

A contribution by Culnan and Bies (2003) considering consumers' privacy proposed that there are three relevant types of justice perceptions to be considered: distributive, procedural, and interactional. Distributive justice deals with the fairness of exchange among parties, where the cost of giving in personal data should be proportionate with what is gained in return. Procedural justice entails the ways in which this sharing of information is enacted and its fairness. Moreover, there should be awareness or knowledge of the procedure. Finally, interactional justice refers to the ways in which consumers are treated interpersonally. In this context, honesty, fulfillment of promises, and unwarranted disclosures of personal information play a role in determining the degree of fairness of interpersonal treatment. Culnan and Bies (2003) then consider that three different approaches can be followed in order to implement fair information practices that meet the requirements of the three types of justice: a) technological solutions; b) self-regulation; and c) legislation and government regulations. Technological solutions aim at allowing individuals control over the disclosure of sensitive personal information and at helping organizations to maintain the privacy over the data acquired by their customers. Two instances are represented by the Platform for Privacy Preferences, mentored by the World Wide Web Consortium, and by the possibility to visit websites anonymously or to decide over one's online identity and cookies, while browsing the web. There are also two types of tools that may be used by firms to conform to privacy policies. The first one considers if the websites have problems with the use of cookies to collect personal information or the absence of links to privacy indications. The second possible set of tools fixes the rules for the firms' databases that cannot be used in conflict with the options that the customers have chosen in terms of preferences for privacy. Culnan and Bies (2003) also discuss the possibility to adopt self-regulation by firms, i.e. the development of specific rules regardless of the public ones. The authors state that, in order for these regulations to generate trust among consumers, there is the need to have enforcement strategies and compliance procedures, particularly by third parties, autonomous from firms, e.g. website privacy seals or trade associations requirements for membership. Lastly, the authors consider that there is a lack of evidence about the effectiveness and implementation of self-regulations. This is one of the reasons that has led to the development of public regulations. The rest of this section will discuss the instances of legislation and government regulations to enhance fair management of online privacy.

One of the most important public regulations about the privacy of online data is definitely the General Data Protection Regulation (GDPR), issued by the European Union in 2016, that came into effect in 2018. The rules contained in the GDPR are applicable to all firms operating within the European Union, even if they are incorporated outside its boundaries (Frey and Presidente, 2024). The main aim of the GDPR was to give individuals control over their sensitive data, also by fostering a limited use of such data for marketing and other economic purposes by the firms who had collected them. Several instances of such limitations are given by the prohibition to share data without the explicit consent of the customer, by the allowance to individuals to access their own data to correct, update, or amend them, and by the obligation to encrypt and anonymize the personal data that a firm has stored. Several studies have been proposed in the last years to try and estimate the economic consequences connected with the implementation of the GDPR by firms. Table 1 lists a summary of the main findings of the research that has been carried out since the inception of the GDPR.

Table 1. GDPR's estimated effects

Authors	Main findings	Implications	Data setting
Jia et al. (2021)	Negative short-term effects on investment in technology ventures. Particularly in the period immediately after the GDPR and for newer, data related and consumer facing ventures	Negative impact on venture capital investment into technology firms	Venture capital investment
Zhao et al. (2023)	GDPR modifies consumers' browsing and search behaviour. A panel of individuals exposed to GDPR has 21.6% more search terms for information and 16.3% more pages browsed for goods and services access with respect to a control group.	GDPR increased friction in online search, that is heterogeneous among firms. Small e-commerce firms are hurt more.	Consumer online browsing, app usage, and search activities
Zhuo et al. (2021)	Economically small or no effect of GDPR: the number of observed agreements, agreement types, the number of observed interconnection points per agreement, the entry, and the observed number of customers of networks.	GDPR had no visible short-run impact on the Internet interconnection layer.	Internet interconnection
Chen (2022)	GDPR gives users the possibility to opt out from providing personal data and to still continue to use the services of the digital platforms.	GDPR causes a reduction in the investment in digital services.	Theoretical model
Godinho de Matos and Adjerid (2022)	Consumer's consent for different data types improved when GDPR compliant consent was obtained, leading to an increase	GDPR may be effective for enhancing consumer privacy protection while at the same time enabling companies to	Large telecommunication provider with operations in Europe

	in sales because of more effective targeted advertising.	improve products that rely on consumers personal data.	
Janssen et al. (2022)	GDPR induced one-third of the available apps to exit and decrease the entry rate of new apps in the market by half.	GDPR reduced beneficial innovation.	Apps on Google Play store
Peukert et al. (2022)	Websites reduce the number of third-party web technology providers they use, including websites not legally bound by the GDPR. The changes are disproportionally pronounced among less popular websites.	All firms experience losses. However, the vendor leader, Google, incurs relatively smaller losses and greatly expands its market share in crucial markets like advertising and analytics.	Web technology industry
Aridor et al. (2023)	The opt-in requirement of GDPR led to a 12.5% decrease in the consumer amount. However, the remaining consumers are trackable and predictable for a longer period of time. Their rising value to advertisers offsets part of the losses.	GDPR-enabled opt-out option increases the trackability of the opt-in consumers who choose to reveal their data, imposing an externality.	Online travel intermediary
Johnson et al. (2023)	After GDPR's enforcement deadline, the website use of web technology vendors decreased by 15% among EU residents. At the same time, the concentration of vendor market increased by 17%, since websites are more likely to drop smaller vendors.	GDPR increased market concentration among technology vendors in a business-to-business context.	Web technology vendors
Frey and Presidente (2024)	GDPR influences firms' performances by adding costs and lowering sales. Increase of investments in privacy technology.	GDPR affects mainly digital firms and the firms which rely on digital firms for their operations.	Multi country and multi sector analysis.
Goldberg et al. (2024)	Reduction of approximately 12% in both website page views and e-commerce revenue among EU users, as recorded by the Adobe's analytics platform after the GDPR's enforcement deadline.	GDPR both reduced data recording and harmed real economic outcomes.	Adobe's website analytics platform

Source: author's elaboration based on Goldfarb and Que (2023)

Several considerations can be drawn from the conjoint analysis of all the listed studies. It appears that the GDPR has implied a reduction of web visits and revenue, of efficiency of online search, of the ability of firms to target consumers, and of the competition in the market (given that the most relevant costs have been brought by small and medium firms). However, it may also be the case that these effects, as highlighted by part of the literature, may be small in magnitude and related to the short and medium term. They would then decay over time.

Another important public regulation of data privacy is the California Consumer Privacy Act, that has been enforced since April 2020, and then modified into the California Privacy Rights Act in November 2020. This regulation provides consumers with the possibility to control how the sensitive information related to them is used, imposes detailed disclosure requirements, creates a private right of action, and poses fines for breaching its obligations. A work by Canayaz et al. (2022) has analysed the effects of this regulation by means of a general equilibrium model. Their results confirm part of those obtained by the literature on the GDPR, namely that firms with AI products perform worse than their competitors and that firms with weak customer bases are hit hardest. What seems to be missing in the literature is an analysis of the benefits generated by the GDPR in terms of development of privacy preserving technologies and analytics, and, especially, of the downstream positive effects on consumers and on society as a whole.

Conclusions

The paper has proposed the main theoretical and empirical findings related to the economic value of privacy. It has also analysed the main public regulations of data privacy emphasizing the effects in terms of market efficiency and of outcomes for firms and individuals. The theoretical review has highlighted that the concept of privacy has undergone a long evolution over time, given its contextual nature. It has emerged that privacy can be considered as a final good, that has a value in itself, but also as an intermediate one that allows to reach specific goals. In this context, the availability to share data is deeply influenced by the trust of individuals in the firms and institutions that manage them. It has also been considered that the disclosure of personal data may provide economic benefits to consumers in terms of better and tailored services, but it also entails the possibility of costs and negative externalities. The optimal amount of privacy should be determined in conjunction with other important values, such as wealth and security. This determines a series of trade-offs both for the data holder and for the economic system as a whole.

The review of empirical findings has allowed to ascertain a clear difference between the willingness to pay to maintain personal data classified and the willingness to accept compensation in order to disclose it. It has also appeared evident that the economic values of privacy are very heterogeneous, and they depend on the specific piece of data, on the geographic, social and economic context and on demographic characteristics of the respondents.

The analysis of the regulations on data privacy and on their economic effects has allowed to infer that they have determined a reduction of web visits and revenue, of efficiency of online search, of the ability of firms to target consumers, and of the competition in the market. Part of the literature has argued that these effects may be small in magnitude and related to the short and medium term. Future research in this context should evaluate the benefits generated by regulations in terms of development of privacy preserving technologies and analytics and the downstream positive effects on consumers and on society as a whole.

Acknowledgement: The author acknowledges the financial support of the Italian PRIN Project n. CUP F53D2301215-0001 (Digital market and consumer protection). He would also like to thank the participants to the International Conference "The transformative economy, digital technology, spatial disparities and quality of life", held in Yerevan (Armenia) on October 8th – 10th 2024, and two anonymous referees for the useful comments and discussions on preliminary versions of the paper.

References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442-492. http://dx.doi.org/10.1257/jel.54.2.442

Anisimov, A., & Ryzhenkov, A. (2021). Current legal issues of digitalization of environmental protection: a view from Russia. *Eastern Journal of European Studies, 12*(2), 105-122. http://dx.doi.org/10.47743/ejes-2021-0206

Aridor, G., Che, Y.-K., & Salz, T. (2023). The effect of privacy regulation on the data industry: empirical evidence from GDPR. *RAND Journal of Economics*, *54*(4), 695-730. https://onlinelibrary.wiley.com/doi/pdf/10.1111/1756-2171.12455

Bansal, G., Zahedi, F.M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*, 1-21. http://dx.doi.org/10.1016/j.im.2015.08.001

Baumann, A., Haupt, J., Gebert, F., & Lessmann, S. (2019). The price of privacy. An evaluation of the economic value of collecting clickstream data. *Business & Information Systems Engineering, 61*(4), 413-431. https://doi.org/10.1007/s12599-018-0528-2

Canayaz, M., Kantorovitch, I., & Mihet, R. (2022). *Consumer Privacy and Value of Consumer Data* (Research Paper No. 22-68). Swiss Finance Institute. http://dx.doi.org/10.2139/ssrn.3986562

Chen, Z. (2022). *Privacy Costs and Consumer Data Acquisition: An Economic Analysis of Data Privacy Regulation* (Discussion Paper No. 2022-07). Monah Business School. http://dx.doi.org/10.2139/ssrn.4085923

Choi, J. P., Jeon, D.-S., & Kim, B.-C. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics*, *173*, 113-124. https://doi.org/10.1016/j.jpubeco.2019.02.001

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323-342. https://doi.org/10.1111/1540-4560.00067

D'Annunzio, A., & Menichelli, E. (2022). A market for digital privacy: consumers' willingness to trade personal data and money. *Journal of Industrial and Business Economics*, *49*, 571-598. https://doi.org/10.1007/s40812-022-00221-5

De Capitani Di Vimercati, S., Foresti, S., Livraga, G., & Samarati, P. (2012). Data privacy: Definitions and techniques. *International Journal of Uncertainty, Fuzziness and*

Knowledge Based Systems, *20*(6), 793-817. https://doi.org/10.1142/S0218488512400247

Frey, C.B., & Presidente, G. (2024). Privacy regulation and firm performance: Estimating the GDPR effect globally. *Economic Inquiry*, *62*, 1074-1089. https://doi.org/10.1111/ecin.13213

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of the literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226-261. https://doi.org/10.1016/j.cose.2018.04.002

Godinho de Matos, M., & Adjerid, I. (2022). Consumer consent and firm targeting after GDPR: the case of a large telecom provider. *Management Science*, *68*(5), 3330–3378. https://doi.org/10.1287/mnsc.2021.4054

Gokmenoglu, K., & Kaakeh, M. (2022). An empirical investigation of the extended technology acceptance model to explain mobile banking adoption. *Eastern Journal of European Studies*, *13*(2), 204-225 http://dx.doi.org/10.47743/ejes-2022-0210

Goldberg, S.G., Johson, G.A., & Shriver, S.K. (2024). Regulating privacy online: An economic evaluation of the GDPR. *American Economic Journal: Economic Policy*, *16*(1), 325-358. https://doi.org/10.1257/pol.20210309

Goldfarb, A., & Que, V.F. (2023). The economics of digital privacy. *Annual Review of Economics*, *15*, 267-286. https://doi.org/10.1146/annurev-economics-082322-014346

Hirschprung, R., Toch, E., Bolton, F., & Maimon, O. (2016). A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior*, *61*, 443-453. http://dx.doi.org/10.1016/j.chb.2016.03.033

Janssen, R., Kesler, R., Kummer, M.E., & Waldfogel, J. (2022). *GDPR and the lost generation of innovative apps* (Working Paper No. 30028). NBER Working Paper Series. https://www.nber.org/system/files/working_papers/w30028/w30028.pdf

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., & Goldberg, S.G. (2023). Privacy and market concentration: Intended and unintended consequences of the GDPR. *Management Science*, *69*(10), 5695-5721. https://doi.org/10.1287/mnsc.2023.4709

Jones, C.I., & Tonetti, C. (2020). Nonrivalry and the economics of data. *American Economic Review*, *110*(9), 2819-2858. https://doi.org/10.1257/aer.20191330

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134. http://dx.doi.org/10.1016/j.cose.2015.07.002

Kourtit, K. (2019). Cultural heritage, smart cities and digital data analytics. *Eastern Journal of European Studies*, *10*(1), 151-159. https://ejes.uaic.ro/articles/EJES2019_1001_KOU.pdf

Lukacs, A. (2016). *What is privacy? The history and definition of privacy*. University of Szeged. https://www.cag.edu.tr/uploads/site/lecturer-files/what-is-privacy-the-history-and-definition-of-privacy-ULpz.pdf

Martin, K. (2020). Breaking the privacy paradox: The value of privacy and associated duty of firms. *Business Ethics Quarterly*, *30*(1), 65-96. https://doi.org/10.1017/beq.2019.24

Moore, A. (2008). Defining privacy. *Journal of Social Philosophy*, *39*(3), 411-428. https://ssrn.com/abstract=1980849

Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T. (2022). Regulatory spillovers and data governance: evidence from the GDPR. *Marketing Science*, *41*(4), 746–768. https://doi.org/10.1287/mksc.2021.1339

Poindexter, J.C., Earp, J.B., & Baumer, D.L. (2006). An experimental economics approach toward quantifying online privacy choices. *Information Systems Frontiers*, *8*, 363–374. https://doi.org/10.1007/s10796-006-9013-4

Posner, R. A. (1981). The economics of privacy. *The American Economic Review*, *71*(2), 405-409. https://www.jstor.org/stable/1815754

Prince, J.T., & Wallsten, S. (2022). How much is privacy worth around the world and across platforms?. *Journal of Economics and Management Strategy*, *31*, 841-861. https://doi.org/10.1111/jems.12481

Savage, S.J., & Waldman, D.M. (2015). Privacy tradeoffs in smartphone applications. *Economic Letters*, *137*, 171-175. http://dx.doi.org/10.1016/j.econlet.2015.10.016

Skatova, A., McDonald, R., Ma, S., & Maple, C. (2023). Unpacking privacy: Valuation of personal data protection. *PLoS ONE*, *18*(5), e0284581. https://doi.org/10.1371/journal.pone.0284581

Solove, D.J. (2011). *Nothing to Hide*: the *False Tradeoff between Privacy and Security*. Yale University Press, New Haven and London.

Tesary, L. (2022). Valuing intrinsic and instrumental preferences for privacy. *Marketing Science*, *41*(4), 663-681. https://doi.org/10.1287/mksc.2022.1368

Van Aaken, D., Ostermaier, A., & Picot, A. (2014). Privacy and freedom: an economic (re-)evaluation of privacy. *Kyklos*, *67*(2), 133-155. https://doi.org/10.1111/kykl.12047

Wang, T., Duong, T.D., & Chen, C.C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*, 531-542. http://dx.doi.org/10.1016/j.ijinfomgt.2016.03.003

Winegar, A.G., & Sunstein, C.R. (2019). How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy*, *42*, 425-440. https://doi.org/10.1007/s10603-019-09419-y

Zhao, Y., Yildirim, P., & Chintagunta, P.K. (2023). *Privacy regulations and online search friction: evidence from GDPR* (Report No. 23-141). Marketing Science Institute Working Paper Series 2023. https://thearf-org-unified-admin.s3.amazonaws.com/MSI_Report_23-%20141.pdf

Zhuo, R., Huffaker, B., Claffy K.C., & Greenstein, S. (2021). The impact of the General Data Protection Regulation on internet interconnection. *Telecommunications Policy*, *45*(2), 102083. https://doi.org/10.1016/j.telpol.2020.102083