Kişisel Verileri Koruma Dergisi
www.kvkk.gov.tr Cilt:5 Sayı:1 Geliş:18.06.2023
Kabul:23.06.2023

The Privacy Paradox Is Not Real

Esra, ÜNAL YEŞİLYURT
University of Kent, UK, Ticaret Bakanlığı, Ticaret Uzmanı,
Ankara, Türkiye
unalessra@gmail.com
ORCID ID: 0000-0001-9252-4589

ABSTRACT
Privacy paradox is the term used to describe the discrepancy between people's claimed privacy preferences and their actual actions towards the security of their personal information. Surveys show that despite increased privacy concerns, consumers frequently voluntarily divulge their personal information without taking the necessary precautions to secure it. The article makes the case that the privacy paradox may not always exist and that people's beliefs and behaviors surrounding privacy may not always coincide due to a number of issues, such as individualized perceptions of privacy and the complexity of risk assessment. The article investigates alternative causes for the observed inconsistencies and critically evaluates various viewpoints on the privacy dilemma. It underlines how important it is to take decision-making processes into account when making decisions and suggests that privacy laws and regulations be changed to take these considerations into account. The article concludes that to create efficient privacy protection mechanisms, it is essential to comprehend the multidimensional nature of privacy and the underlying motivations behind people's activities.
Keywords: privacy paradox, privacy preferences, risk assessment, decision-making processes, privacy laws.

Gizlilik Paradoksu Gerçek Değil

ÖZ
Gizlilik paradoksu, insanların iddia ettikleri gizlilik tercihleri ile kişisel bilgilerinin güvenliği konusundaki gerçek eylemleri arasındaki tutarsızlığı tanımlamak için kullanılan bir terimdir. Anketler, artan gizlilik endişelerine rağmen, tüketicilerin sıklıkla kişisel bilgilerini istekli bir şekilde paylaştıklarını, bunları güvence altına almak için gerekli önlemleri almadıklarını göstermektedir. Makale, gizlilik paradoksunun her zaman var olmayabileceğini ve gizlilikle ilgili inançlar ve davranışların bireyselleştirilmiş gizlilik algıları ve risk değerlendirmesinin karmaşıklığı gibi birçok sorun nedeniyle her zaman uyumlu olmayabileceğini savunmaktadır. Makale, gözlenen tutarsızlıklar için alternatif nedenleri araştırmakta ve gizlilik sorunuyla ilgili çeşitli görüşleri eleştirel bir şekilde değerlendirmektedir. Karar verme süreçlerini dikkate almanın önemini vurgulayarak, gizlilik yasalarının bu hususları dikkate alacak şekilde değiştirilmesini önermektedir. Makale, etkili gizlilik koruma mekanizmaları oluşturabilmek için gizliliğin çok boyutlu doğasını ve insanların eylemlerinin temel motivasyonlarını anlamanın önemli olduğu sonucuna varmaktadır.
Anahtar kelimeler: gizlilik paradoksu, gizlilik tercihleri, risk değerlendirmesi, karar verme süreçleri, gizlilik yasaları.

Atıf Gösterme Ünal Yeşilyurt, E. (2023). The Privacy Paradox Is Not Real, *Kişisel Verileri Koruma Dergisi. 5*(1), 47-56. DOI:

INTRODUCTION

In the current digital era, privacy has grown to be a major worry. In terms of gathering, preserving, and exchanging personal information, the internet and other technological developments have created new difficulties. Thanks to technological improvements, many surveys show that individuals are increasingly concerned about their privacy nowadays (Kokolakis, 2017, p. 122). Since people's private information can be used by companies to profit for commercial reasons, or it can be used for surveillance by the governments, people find themselves in situations to protect their private life and personal data.

Growing conversations and arguments over data protection laws, privacy rights, and the moral implications of data gathering and use have taken place in recent years. Governments, businesses, and individuals are all actively looking for solutions to protect personal data and create effective privacy frameworks. Therefore, although there is no specific definition of privacy, many legislations and restrictions have been put in place to protect people's privacy and data. The European Union (EU) safeguarded privacy and data protection through the Treaties and the EU Charter of Fundamental Rights and regulated data privacy detailed in the General Data Protection Regulation to protect citizens.

Although the privacy of personal information is a crucial concern worldwide, most people rarely take action to secure their info and frequently give it away voluntarily, according to some surveys (Gerber et. al., 2018, p. 226). The disparity between privacy actions and behaviour is commonly known as the "privacy paradox." While theoretical and empirical studies look for answers to the privacy paradox, no thorough analysis of the privacy paradox has yet been discovered (Gerber et. al., 2018, p. 226).

Some researchers try to explain the privacy paradox by claiming that people's behaviour more accurately reflects their privacy values than their expressed opinions, while others contend that people's behaviour is illogical or inconsistent with their true preferences because behaviour is not a reliable indicator due to distortions such as manipulative aspects (D. Solove, 2020, p. 1). However, some scholars claim that the privacy paradox cannot be explained so far because it does not exist at all (D. Solove, 2020, p. 2). The existence of the phenomena is just a deception generated by flawed logic and unjustified generalisations. Within this context, they make suggestions about how the law should be regulated or amended based on their perspectives.

Overall, this article argues that there is no privacy paradox, and people's attitudes and behaviours do not have to be consistent because preferences are only about risk assessments, and the value of privacy is a broad concept that cannot be understood by a restricted empirical study. However, distortions also should be considered because we cannot assume people make decisions based on fully rational risk assessment all the time. In the first part of the article, the concept and definition of privacy, which is the key element for the privacy paradox, is tried to be explained. The current surveys about the privacy paradox will be put in place in the second part, and the two main perspectives about the paradox will be discussed in the third part. In the fourth part, the idea that sees the privacy paradox as a myth will be critically assessed. The last part will analyse how the privacy law should be regulated and amended.

PRIVACY AS AN AMBIGUOUS CONCEPT

The term "privacy" has a lot of diverse implications and numerous forms in legal, policy making, moral, social studies, arts, the media, and the internet (Francis & Francis, 2017, p. 2). Technological improvements such as camera systems, CCTV, the internet, and biosensors make surveillance and interference easier on people who face persistent challenges to privacy and its meaning. There is a variety of meanings, indicating uncertainty about whether privacy is a psychological condition, a form of control, a right, a claim, or freedom not to partake (Parker, 1973, pp. 275-276). A conception of privacy is a mental image of what privacy is and what makes it special (D. J. Solove, 2008, p. 13).

Some may define privacy as "limited access" to one's self, which acknowledges an individual's desire for privacy and separation from others (D. J. Solove, 2008, s. 18). It can be a psychological condition of being estranged from others (Weinstein, 2017, s. 88). Some may consider it as a sort of power of managing personal data and controlling the spread of information about them (Josephson, t.y., p. 1391), which is a claim or right to control when, with whom, how, and to what extent information is shared with others, or having a right not to participate in other people's actions. (Westin, 1968, p. 24) Or, it can be seen as a right to hide the disgraceful facts about themselves (Posner, 1978, p. 1), which can be

conceptualised under secrecy (D. J. Solove, 2008, s. 21). Similar to these ideas, the concept of intimacy considers our ability to manage who has access to us and knowledge about us and our ability to build and maintain various types of social interactions with various people (Rachels, 1975, p. 332).
Another view of privacy is that it is a means of preserving persons, and it is built around a normative purpose of privacy, namely the preservation of personality integrity, which can be related to autonomy (D. J. Solove, 2008, pp. 29-30). Some may propose a different definition of privacy as a right to be free of bodily, mental, or spiritual harm (Henkin, 1974, p. 1411). The right to privacy is commonly viewed as the ability to be left alone by others, which safeguards an individual's privacy from the government, corporations, and fellow citizens, focusing on the right to deny them access to one's information, body, or residence (Sloot, 2021, p. 223).
As can be seen from these theories, there are various perspectives trying to understand what the concept of privacy really means and that privacy encompasses a wide range of interconnected concepts. However, the theories are either too narrow or too broad; therefore, no precise definition of privacy is accepted worldwide. One of the reasons privacy appears so difficult to define is that its criteria are frequently framed in terms of expectations. (Francis & Francis, 2017, p. 16)
Even if there is no commonly agreed definition of privacy, and people might conjure up their ideas about it, people nonetheless place a high value on their privacy. The value of privacy stems from the fact that the loss of privacy comes with violating most of one's other fundamental rights and freedoms. (Parker, 1973, p. 287) Privacy is considered a basic human right and privacy rule in Europe, and Article 8 of the European Convention on Human Rights states that respect for private and family life is guaranteed.
While trying to understand its value for people, we can find solutions depending on different aspects such as culture, expectations, circumstances, and concrete cases. Therefore, it can be argued that the relevance of privacy to society must be considered rather than individual rights when determining its value (D. J. Solove, 2008, p. 10). The social importance of the activities that privacy facilitates can determine the value of privacy in each situation because privacy does not have a universal value that applies to all situations (D. J. Solove, 2008, p. 10).
Overall, the notion of privacy includes a wide range of elements, and the value of privacy, or how people interpret the term or what they want to preserve with their personal information, is highly subjective. As a result, this fact should be addressed when examining the privacy paradox when examining if it is a myth or not.

THE CONCEPT OF THE PRIVACY PARADOX

There have been many surveys to search for people's attitudes and behaviours in given different circumstances. It has been observed that even those who value their privacy are willing to sell privacy for convenience or negotiate the release of extremely personal data for a small fee. A study in 2001 stated that the participants looked eager to offer generic concerns about privacy, but they were also willing to give up that privacy for very little value, which may appear to be something of a paradox (Brown, 2001). Participants were invited to answer a survey on privacy attitudes and preferences before visiting an online business in another study to show self-reported privacy preferences with real disclosing behaviour during online purchasing. Although online users state that privacy is a major issue, their actions do not reflect this, as evidenced by the fact that they answered most questions, even if they were incredibly personal (Spiekermann et. al., t.y., pp. 39, 45).
Barnes (Barnes, 2006) further elaborated the concept of privacy, and it is stated that a large amount of info shared online, the illusion of privacy on social networking sites, and the disconnect between context and behaviour indicate that even when people recognise that social networking sites are public spaces, they still act as if they are private, and users' lack of understanding of information processing efforts by online businesses.
Researchers using the behavioural economics approach gave more evidence of an attitude vs behaviour split as well as some tentative explanations of the phenomena such as Acquisti and Grossklags found that while 89.2 percent of respondents said they expressed concern about privacy in some way, 21.8 percent agreed to give their social security numbers in exchange for discounts, better services, or recommendations, and 28.6 percent supplied their phone numbers. Many participants admitted to not using certain privacy-protecting procedures when their activity was examined (Acquisti & Grossklags, 2005, pp. 28-29).

In Acquisti and Gross's study about social media, even though nearly 77% of respondents claimed they had not read Facebook's privacy policy, and many of them inaccurately assumed that Facebook does not collect (67%), combine (70%), or share (56%) information about them. In addition, according to the responders, individuals who are not connected with a university find it impossible or extremely difficult to gain access to the university's Facebook network. Therefore, inconsistency between concern and disclosure can stem from a lack of awareness of Facebook's privacy rules, trusting the company, or psychological motives (Danezis & Golle, 2006, pp. 53-57).
The abovementioned study also mentions another research that finds growing public concern about online social network privacy threats affecting some of their users (Danezis & Golle, 2006, p. 57). Conversely, a survey discovered that having more knowledge did not lead to more privacy-protective behaviour (Barth et. al., t.y., s. 65). It was an experiment to see how many technically savvy students would download and use a mobile phone app if they were given enough money to buy a paid-for app. Consumers have expressed concern about the probable improper use of their personal data; however, they are hesitant to devote the time, effort, or cost required to preserve their privacy despite having technology expertise and a better-than-average understanding of privacy invasion threats (Barth et. al., t.y., p. 65).
A study showing privacy paradox has found that only 35.4 percent of those surveyed would spend a price to get a version of their online mail service that did not employ automatic online mail content analysis to deliver personalised adverts. The median readiness for a payment was $15 per year among nearly one-third of the participants ready to pay a sum of money, while only 3% of the respondents said they were willing to spend over $120 each year for a such e-mail service (Strahilevitz & Kugler, 2016, p. S78). Even in a survey, it has been found that most subjects were willing to sell their personal information for as little as 25 cents and that almost everyone waived the choice to keep their information private (Grossklags & Acquisti, t.y.).
The privacy paradox has massive repercussions for e-commerce, e-government, web-based platforms, and government privacy legislation (Kokolakis, 2017, p. 122). In commercial, legal, and regulatory contexts, the economic worth of personal information is important as an objective standard of value (Lim, 2021, s. 244). Large volumes of personal information are collected by electronic commerce and social media platforms; therefore, a demonstration of the privacy dilemma would compel them to expand the acquisition and utilization of private data. On the other hand, government policymakers defend privacy legislation by citing people's expressed privacy concerns, and the privacy paradox can damage the justification (Kokolakis, 2017, pp. 122-123). For these reasons, it is crucial to understand if the phenomenon exists or what brings the inconsistency between people's attitudes and behaviours.

TWO MAIN PERSPECTIVES ACCEPTING THE PRIVACY PARADOX

Some scholars believe the privacy paradox is a fact-based on different arguments and perspectives. Solove categorises them in two: People's revealed attitudes, according to the "behaviour valuation argument", are a better indicator of their true preferences than their stated choices. Therefore, regulation should focus on behaviours because the privacy paradox shows that individuals place a low value on privacy or are willing to sell it for goods and services (D. Solove, 2020, p. 8). According to the "behaviour distortion argument", people's true privacy preferences may not be reflected by their behaviours because they may be distorted by certain elements such as heuristics and biases, framing effects, manipulation, lack of knowledge, inertia, and friction (D. Solove, 2020, p. 11). Thus, regulation should focus on removing the distortion elements affecting people's choices.
Heuristics and biases can cause people to behave in this way because they impair people's capacity to evaluate their options rationally, resulting in certain decision-making issues. People usually make conclusions based on data of poor validity that has been processed using heuristic criteria such as the presumption of the perceived distance (Tversky & Kahneman, 1974, p. 1124). Heuristics are cost-efficient and usually effective, yet they lead to foreseeable and recurring errors. Therefore, gaining a greater understanding of these heuristics and the biases that they cause could aid people in making better determinations of uncertain circumstances (Tversky & Kahneman, 1974, p. 1131).
A study shows that people's desire to share private data can cause the feeling of having a fictional sense of control (Brandimarte et. al., 2013, p. 345). Three tests in this study show that in comparison to the objective hazards involved with others' access to and use of information, perceived control over release

plays an important role in sharing/oversharing personal information. Control is regarded as an important aspect of privacy, and several government and corporate institutions in the US have pushed for self-regulatory "choice and consent" privacy models that rely on users' understanding and control (Brandimarte et. al., 2013, p. 346). However, the study reveals that control can affect the opposite effect. Another cause for paradox can be technological design. The system has been constructed to maximize collection, maximize visibility, and ensure that everything is always available, which all works for the company's interests and against the benefits of the consumers. (Vaidhyanathan, 2012, p. 84) People need to understand how the system works to manage their global electronic profile. Or the explanation can be the technology itself. The internet makes it easier for people to share information without ordinary features that can make them entirely understand the outcomes because technology changes how people live and act (D. Solove, 2020, p. 14).

People's knowledge is often limited and/or mistaken. Consumers mistakenly believe that restrictions prohibit the use and sale of personal information, leading to a privacy dilemma (D. Solove, 2020, p. 15). It has been discovered in a study that when participants were given important privacy information, they took it into account when making purchases from websites with medium or high degrees of privacy (Tsai et. al., 2011). In the study, people were invited to go shopping for batteries, and a vibrator from different online shops giving different privacy protection information, and people paid more for one store with privacy information than others. Therefore, it has been suggested that contrary to popular belief, consumers might be ready to pay a premium for privacy. Yet, the difference between online shops with different knowledge was quite low: 0.62 USD (D. Solove, 2020, p. 35).

Also, most people can be unwilling to safeguard their privacy, and they do not manage their privacy settings. (D. Solove, 2020, p. 16) When people use online services, especially social networks, the term "friction" refers to the forces that prevent them from giving personal information (McGeveran, 2015, p. 15). Companies can purposefully increase the friction for people to make privacy-protective choices, leading to a change in behaviour. The more difficult it is to modify privacy settings, opt-out, and apply other privacy-protecting measures, the less likely people are to do so. As a result, friction might become privacy's greatest threat, so the correct amount of friction, rather than its eradication, should be the goal (McGeveran, 2015, p. 18)

DOES THE PRIVACY PARADOX REALLY EXIST?

Solove argues that the behaviour in the privacy paradox research is about preferences that incorporate risk evaluations in contexed scenarios. (D. Solove, 2020, p. 18) But people's views about privacy are frequently described in broad terms that apply to a variety of situations. As a result, there is no conflict between behaviour and attitudes because they are concerned with entirely distinct issues. Privacy paradox research on behaviour entails a risk-based decision in a very specific situation, and the results are founded on erroneous generalisations about people's actions. The possibility of danger or loss is considered a risk, while the entire importance that a person ascribes to anything is considered value. (D. Solove, 2020, p. 19)

Within this context, he contends that there is a distinction between how much people appreciate their privacy and, in general terms, because even if they do not care about their privacy, they might value privacy in general, considering the good for all. Also, many studies accepting the privacy paradox do not reveal that people do not care about their privacy; instead, they reveal that people are making decisions that may jeopardise their privacy (D. Solove, 2020, pp. 20-21). It can be claimed that behaviours are unique and dependent on the situation (Acquisti et. al., 2016, p. 477). Therefore, it's not unusual that the former does not always correspond to or anticipate the latter. Also, attitudes are frequently articulated in broad terms, so it can be argued that a dilemma does not exist at all.

Confounding variables can affect studies (Martin & Nissenbaum, 2017, p. 176). A design that concentrates on only one of the norm-defining criteria or open-ended questions can lead to unclear results or false presumptions of respondents. People's willingness, even eagerness, to disclose, distribute, and exchange information is perfectly compatible with a high value placed on privacy as long as the information flows are proper. If the flow is right, giving up information, no matter how much, is not the same as giving up privacy. When information is exchanged, privacy is not compromised. (2017, p. 191) Privacy is about what a person wants to protect and disclose at any given time and in any particular situation. Thus, sharing specific information does not mean they lose their privacy, and there

is no need for complete concealment of data to protect privacy. In fact, the evidence that customers do not appear to safeguard their privacy very fiercely online does not imply that they never do so (Acquisti et. al., 2016, p. 477).

People may have quite differing viewpoints about privacy when they express their concerns (D. Solove, 2020, p. 22). The inconsistency between expressed intentions and behaviour may result from the incorrect belief that the expressed preference includes the risks that the behaviour entails. People's expressed preferences do not have the same level of specificity as their observed behaviour, such as some may care about their data protection rather than surveillance, while for some, it is the opposite, or what kind of information is more important for them not to disclose. Also, people may make risky decisions in a variety of ways at different times in their lives.

It can be claimed that people that seek privacy do not want to keep their information hidden from everyone; instead, they want to share it judiciously and ensure that it is not misused. With all the technological improvements, it is almost impossible to hide all your information, so privacy does not have to be all-or-nothing; it can be modulated, and data flow can be controlled (D. Solove, 2020, p. 23) Therefore, people are more comfortable sharing personal data with businesses or engaging in e-commerce when privacy regulations are in place because they trust the privacy rules and laws that our personal information will not be misused. So, one may claim that privacy regulations may cause more data flows than prevent misuse. (D. Solove, 2020, p. 25)

Privacy is a highly contextual concept (Kokolakis, 2017, p. 127). Our privacy valuation is a broad context; on the other hand, our behaviour in a specific situation is a very limited area. Thus, it is difficult to understand the attitude and behaviour relation looking at these studies, which are only making risk-based decisions on a limited subject. People are acting rationally whether to share private information on a risk-based approach, and if they share their data with a specific shop, service, or person does not mean they do not value it in general. Or, if people give away their limited data, for instance, their address and education info, it does not mean that they may want to share their sexual preferences, which may seem more private or confidential. In addition, people have to manage their privacy settings for cookies every time they try to use a website, but it is mostly time-consuming, and sometimes we have to accept cookies to access the website. So, none of these leads us to the conclusion that people do not care about their privacy in general.

According to one study, people who were more concerned regarding their privacy transferred fewer personal data about them online (Dienlin et. al.., 2021, p. 16). It has been mentioned that privacy concerns and behaviour should be slightly correlated; however, the exact level of this correlation relies on various boundary conditions. But also, it has been emphasised that using alternate techniques to the privacy paradox in other scenarios will almost certainly yield different conclusions.

Having said that, it is difficult to deny distortion effects on people. Technological designs, heuristics, and biases can change people's behaviour. People must share their data because of technological designs, the illusion of having control of their data due to the existence of laws, or simply to use a website. Of course, the main difference between the distortion argument and Solove's suggestion is whether attitudes and behaviours should be consistent or not. From all these explanations, we cannot expect it to be consistent. However, distortions should still be considered in the privacy context, especially while regulating privacy laws to control technological designs rather than giving more control to people.

POSSIBLE LAW AMENDMENTS AND IMPLICATIONS

Consumer surveys that demonstrate a growing breach of personal privacy may prompt requests for legislative intervention because they suggest that consumers routinely submit their personal information (Norberg et. al., 2007, p. 119). So, should privacy regulations be reduced, give people more power to control their data, or bring more sanctions and supervision on collecting and sharing data for companies and governments?

Scholars who support the behaviour valuation argument believe that people's actions show that they do not value privacy so much, whereas privacy regulations place excessive importance on it; thus, they should be reduced. They also frequently seek to make arguments for privacy regulation using estimations of the monetary value of personal data. However, privacy and privacy legislation cannot depend upon individual attitudes and behaviours. It is a broad term determined by its contribution to

democracy, personal well-being, social structure, freedom of expression, and belief. Therefore, it cannot be solely addressed by the market, and the law has a key role in privacy (D. Solove, 2020, p. 28).
For the behaviour distortion argument, if distortive elements can be taken away, maybe by educating people, the inconsistency will disappear. Within this context, people can be able to control their privacy settings and preferences. However, it can be contended that changing the conditions to encourage people to take greater precautions to protect their privacy will not solve the problem (D. Solove, 2020, pp. 36-37). A study shows that reading privacy policies takes an average of 40 minutes per day, based on a point estimate of 244 hours per year per individual (McDonald & Cranor, 2008, p. 563). So, there will be too much work for people to protect their privacy, and giving them more duties may not make it better.
According to an FTC report, it is uncertain if customers even recognise that their information is being gathered, aggregated, and utilized to send advertisements. (Federal Trade Commission, 2008, p. 11) It may be easier to persuade consumers to read policies in shorter times by reducing the length of the terms and conditions (McDonald & Cranor, 2008, p. 567). Current disclosure laws are insufficient, and while adding additional information to policies that the majority of consumers do not read promotes transparency, it may not be realistic (McDonald & Cranor, 2008, p. 568). The California Consumer Privacy Act of 2018 is one example of a privacy regulation that tries to safeguard privacy by providing consumers with more privacy self-management. Within this act, consumers can seek information about their personal data from businesses that obtained them and have the option to opt-out of having their data sold to third parties. But there are other companies that consumers are not aware of collecting their data. Also, consumers can only learn what kind of information is being gathered about them, whereas privacy concerns frequently revolve around how that information will be utilised (D. Solove, 2020, pp. 38-39).
Privacy is a communal endeavour that necessitates the involvement of humans, such as those we engage with on social media, in addition to the technological abilities of social media platforms themselves. One research shows that the inclusion of both a lack of risk awareness and the employment of privacy-protective activities implies that the privacy paradox is unable to be articulated purely by a lack of comprehension or desire for privacy (Hargittai & Marwick, 2016, pp. 3752-3753). Instead, participant responses imply that consumers are apathetic or cynical about internet privacy, believing that data breaches are unavoidable and that opting out is not an option. Participants used a variety of privacy-protective behaviours, but they realised that the aforementioned were likely ineffective in the light of online data mining, widespread theft of identities, constantly shifting privacy settings. Therefore, it is not paradoxical for people to share information when there is not enough protection for them at all. Thus, regulating self-management privacy rules may not bring solutions because it will bring more work for people, and it will not be a type of control or power at all. Instead, organisations and governments should pay attention to privacy scepticism considering it could lead to a psychological comprehension that is not founded on a disconnect between attitudes and behaviour instead focusing on attitudes adapting to perceived conditions, avoiding cognitive dissonance (Hoffmann et. al., 2016).
It can be suggested that instead of making self-management privacy regulations, certain sorts of personal data transfers should be banned, or privacy regulations may render them more difficult. Also, the provisions of the contracts for the transfer of personal data to other parties can be regulated by privacy legislation, and a strong governance strategy with proper institutions can play a key role in protecting privacy. Privacy rules can be regulated by banning designs that could harm customers or developing mechanisms against the dangers of new technologies. It can bring rules for responsible institutions to investigate suspicious new technological devices before going to market or bring regular inspections for websites, products, or services. It is important for regulations to set limits on data collection and usage by prohibiting it when it goes beyond people's reasonable expectations or when it is unjust or possibly harmful.

CONCLUSION

In today's digital age, privacy has become a crucial problem. Due to the quick development of technology and the expansion of digital platforms, there are now many threats that might affect the security of personal information. Although the user data security procedures now in place have improved, there are still issues. There is no single accepted definition of privacy due to its complexity.

It incorporates a range of viewpoints, including restricted access to oneself, controls over one's personal data, the right to keep some information private, and the maintenance of one's integrity as a person. The importance of privacy is extremely individualized and influenced by cultural, social, and personal variables.

Privacy paradox has been tried to be understood by surveys and research for many years. Some have found that privacy dilemma exists due to inconsistency between people's attitudes and behaviour about their privacy. However, another approach claims it is not a reality considering privacy is a broad and contextual concept, and attitudes and behaviour do not need to be in the same direction.

The privacy paradox is viewed from two basic approaches. Both the behaviour valuation argument and behaviour distortion argument views argue that attitudes and behaviour should normally be parallel. According to the behaviour valuation argument, people's exposed attitudes and behaviours are a good indicator of their genuine preferences since they show how little value they place on privacy. This viewpoint holds that regulations should be more concerned with actions than preferences. For this argument, despite the fact that people claim they care about privacy, they do not act that way; therefore, privacy rules should be lessened. The behaviour distortion concept, on the other hand, contends that due to elements like heuristics, biases, manipulation, and ignorance, people's activities might not correctly reflect their genuine privacy preferences. According to this viewpoint, distortions have an impact on the decision-making process, so the laws should focus on removing these distortions.

Solove suggests a new approach to paradox claiming that attitudes and behaviour do not have to be consistent because the attitude which is the value of privacy is a broad concept while the behaviour which is sharing data on a specific subject is limited; therefore, the value of privacy cannot be understood by surveys focusing on behaviours. He states that people make preferences by making a risk assessment and choosing if it is worth sharing their personal data in these contexts. So, he assumes that people are somewhat rational when making choices.

It can be suggested that paradox does not exist because the term and the value of privacy are too broad and contextual, so it cannot be explained by looking at the results of the surveys. However, we cannot always assume people act rationally and make sophisticated risk assessments every time they make a decision about their private data. The attitudes and behaviour do not have to be consistent, but distortions can also play significant effect in people's behaviour. Therefore, the approach of Solove can be a better explanation; however, the distortion aspects should also be taken into consideration. For privacy regulation, instead of giving too much power to consumers to control their data, it should focus on restrictions for collecting, using, and sharing data for companies and governments. The privacy rules should remove distortions, and even if people are given some control over their data, it should be easier so that they do not have to spend too much time.

Even if there may not be a clear solution to the privacy paradox, it is crucial to take into account both points of view and the many variables that affect people's privacy-related decisions. The regulation of privacy should support knowledge, education, and user control while taking into account the complexity of privacy values and the necessity of overcoming distortion factors. In order to create effective privacy laws and practices, it is critical to find a balance between privacy protection and the advantages of technical breakthroughs and societal demands.

Future privacy-enhancing technology will require constant study, development, and advancement. Furthermore, it is essential to educate people about privacy dangers and give them the information they need to make wise choices about their personal information. We can encourage a more secure and reliable digital ecosystem for all users by putting privacy first. In general, managing the difficulties of privacy in the digital age and making sure that people's privacy rights are appropriately maintained depends on a knowledge of the privacy paradox.

BIBLIOGRAPHY

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security Privacy*, *3*(1), 26-33. https://doi.org/10.1109/MSP.2005.22

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

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*. https://doi.org/10.5210/fm.v11i9.1394

Barth, S., D.T. de Jong, M., Junger, M., Hartel, P. H., & Roppelt, J. C. (t.y.). Putting the privacy paradox to the test_ Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources | Elsevier Enhanced Reader. *Telematics and Informatics*. https://doi.org/10.1016/j.tele.2019.03.003

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, *4*(3), 340-347. https://doi.org/10.1177/1948550612455931

Brown, B. (2001). Studying the internet experience. *Hewlett Packard*. https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf

Danezis, G., & Golle, P. (Ed.). (2006). *Privacy enhancing technologies: 6th international workshop, PET 2006, Cambridge, UK, June 28-30, 2006: revised selected papers*. Springer.

Dienlin, T., Masur, P. K., & Trepte, S. (2021). A longitudinal analysis of the privacy paradox. *New Media & Society*, 1-22. https://doi.org/10.1177/14614448211016316

Federal Trade Commission. (2008). Protecting Consumers in the Next Tech-ade: A Report by the Staff of the Federal Trade Commission. *A Report by the Staff of the Federal Trade Commission*, 50.

Francis, J. G., & Francis, L. (2017). *Privacy: What everyone needs to know*. Oxford University Press.

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

Grossklags, J., & Acquisti, A. (t.y.). *When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*. 22.

Hargittai, E., & Marwick, A. (2016). "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*, *10*(0), Art. 0.

Henkin, L. (1974). Privacy and Autonomy. *Columbia Law Review*, *74*(8), 1410-1433. https://doi.org/10.2307/1121541

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4), Art. 4. https://doi.org/10.5817/CP2016-4-7

Josephson, M. S. (t.y.). Miller: The Assault on Privacy. *Michigan Law Review*, *69*, 10.

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

Lim, S. (2021). Tackling Privacy Paradox: Protecting Right to Self-determination of Personal Information by Estimating the Economic Value of Personal Information and Visualizing the Price. *International Journal of Internet, Broadcasting and Communication*, *13*(2), 244-259. https://doi.org/10.7236/IJIBC.2021.13.2.244

Martin, K., & Nissenbaum, H. (2017). Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables. *Columbia Science & Technology Law Review*, *18*, 176-218.

McDonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*, 543.

McGeveran, W. (2015). The Law of Friction. *University of Chicago Legal Forum*, *2013*(1).

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Parker, R. B. (1973). A Definition of Privacy. *Rutgers Law Review*, *27*(2), 275-297.

Posner, R. A. (1978). Privacy, Secrecy, and Reputation. *Buffalo Law Review*, *28*(1), 1-56.

Rachels, J. (1975). Why Privacy is Important. *Philosophy & Public Affairs*, *4*(4), 323-333.

Sloot, B. van der. (2021). The right to be let alone by oneself: Narrative and identity in a data-driven environment. *Law, Innovation and Technology*, *13*(1), 223-255. https://doi.org/10.1080/17579961.2021.1898315

Solove, D. (2020). The Myth of the Privacy Paradox. *GW Law Faculty Publications & Other Works*.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Spiekermann, S., Grossklags, J., & Berendt, B. (t.y.). *E-privacy in 2nd generation E-commerce | Proceedings of the 3rd ACM conference on Electronic Commerce*.

Strahilevitz, L., & Kugler, M. (2016). Is Privacy Policy Language Irrelevant to Consumers? *The Journal of Legal Studies*, *45*, S69-S95. https://doi.org/10.1086/689933

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, *22*(2), 254-268. https://doi.org/10.1287/isre.1090.0260

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, *185*(4157), 1124-1131.

Vaidhyanathan, S. (2012). *The Googlization of everything: And why we should worry*. University of California press.

Westin, A. F. (1968). Privacy and freedom. *The Washington and Lee Law Review*, *25*(1).