information

Article

Attention Paid to Privacy Policy Statements

Tomáš Sigmund

Faculty of Informatics and Statistics, Prague University of Economics and Business, 130 67 Prague 3-Žižkov, Czech Republic; sigmund@vse.cz

Abstract: The article deals with the topic of attention paid to online privacy policy statements by university students. Privacy policy statements were originally intended to mitigate the users' privacy con-cerns and support trust, but users disregard them. The article uses the theory of planned behav-iour combined with privacy calculus to find and verify determinants of reading privacy policy statements. We used the survey method and evaluated the results with partial least square struc-tural equation modelling. We concluded that the attitude towards reading privacy policy state-ments is influenced by privacy risks and privacy benefits. The intention to read privacy policy statements is influenced by social norms, understanding the privacy policy and mainly by the willingness to spend time and effort reading the statements. The effect of attitude was also signif-icant, but its size was smaller. Finally, wider conclusions are drawn, as the confusion around pri-vacy policy statements is a symptom of a wider social change in the information society.

Keywords: privacy policy statement; privacy calculus; privacy online; online services; understanding privacy policy statements

check for updates

Citation: Sigmund, T. Attention Paid to Privacy Policy Statements. *Information* **2021**, *12*, 144. https://doi.org/10.3390/info12040144

Academic Editor: Xavier Bellekens

Received: 14 February 2021
Accepted: 23 March 2021
Published: 29 March 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Private Information

The aim of this study is to identify and describe factors that influence the approach towards privacy policy statements. The factors determine the intention to read the statements and the execution of this intention.

In the area of web services, the potential for growth is very high because of Internet availability, low access costs, higher computer competence among users, availability of information, processing potential of ICTs (Information and Communication Technologies), personalisation of services and their convenience. On the other hand, users leave behind a lot of personal data which can easily be collected, compiled, used for manipulation or sold.

Culnan (2019) [1] sees big data as the currently most threatening challenge for privacy policy as complex technologies, new data practices and ways of business operations and behavioural advertising are difficult if not impossible to explain in detail. Rapid changes make any privacy notice obsolete and inaccurate. Another problem lies in the secondary use of data. Data may be used for purposes different from those originally stated, they may be combined with data from other sources, new personal data may be created from nonpersonal data. The understanding of contextual norms by companies is limited, even though they are important as they reflect expectations of acceptable practices in various contexts.

We should realise that the original equivalence model of companies' offers and users' choice is not valid any more. The asymmetry is immense, users are very vulnerable and depend on how fairly companies deal with their personal data. Users often can either accept the privacy policy or not receive access to the site or service. That exerts pressure on them and impedes free decision-making.

One option would be if companies integrated ethics and consumers' expectations into their risk assessment, but that is difficult to expect as a lot of data processing is done in secrecy—users very often do not know who uses their data and how they are used. The

benefits of personal data processing for companies are numerous. Another problem dwells in the fact that ethics is not unanimous and transformable into algorithms.

For companies, the information users disclose online represents a source of competitive advantage. Users' information allows companies to understand users' behaviour and preferences. On the other hand, users have concerns regarding their privacy that should be addressed because violations of users' privacy bring reputational damage.

Big data change our decision making [2]. New ICTs allow for collecting, storing and processing big amounts of users' data and subsequently understanding users' behaviour and preferences. Such knowledge provides companies with competitive advantages—companies may personalise their products and services [3].

For users, however, the privacy remains a salient factor [4–7]. They are concerned about information risks [8].

Previous research has focused on variables such as privacy concerns, trust, information sensitivity, intention to disclose personal information [9–11], but it has not focused on privacy policy statements specifically and the application of behavioural theories explaining users' attitude towards them.

Privacy policies inform users about how their personal data will be used and how protected the data will be [12]. The privacy policy should reduce users' fears about their personal information [13].

However, for users, the privacy policy does not represent a simple solution. Privacy policies rely on the principle of transparency, but this solution is not problem-free.

2. Privacy Policy Statement

To increase users' trust web service providers can employ a lot of mechanisms that ensure the personal information will remain secure. Examples include approval of third party certifications, quality of the web site design, ratings, references, financial compensations for privacy breach or privacy policy statements. The statements codify how personal information will be used. They are relatively simple and cheap and help especially in cases where the service provider does not have a high reputation yet. Privacy policy statements vary in length, ease of understanding, placement and level of protection [14]. We will concentrate on privacy policy statements to evaluate their effectiveness and the problems related to them. We will use them as paradigmatic examples of information society changes. The method of scientific literature research and analyses will be used, and synthetic conclusions will be drawn.

As for privacy policy statements, we need some universal rules that would somehow balance the situation even though they will not be able to respect individual differences. The internationally recognised and thus most general principles of information privacy although less detailed than OECD or EU principles (the most famous is the GDPR—General Data Protection Regulation, EU 2016/679) are the FIPP (Federal Trade Commission's Fair Information Practice Principles) practices. These principles form the foundation of privacy statements, which are then supplemented according to the specific circumstances and contexts.

Ignorance of Privacy Policy Statements

The most significant problem with privacy policy statements is that users do not read them. As early as in 2006 T. H. Cate in her book chapter [15] pointed out that the amount of notices and consent opportunities rise, but the public ignores it. An older study has shown that consumers do not even read important information regarding the transaction, such as product warranties [16]. Therefore, although privacy policy statements are well written they do not have any effect if users do not take notice of them. Agreeing with the terms and conditions is very often a fictitious answer. There are even ironic web pages (https://tosdr.org/or@BiggestLie_com, accessed on 24 March 2021) pointing out the hypocrisy. The notice policy does not work. From one perspective it may seem that ignoring the privacy and terms of service policies is a regulatory failure and we need

another, maybe more pragmatic approach that would secure privacy and proper handling of data.

A recent study [17] has shown that 74% of respondents skipped privacy policy statements or terms of service statements. Most respondents agreed to the policies (97% to privacy policy, 93% to terms of service). The negative predictor of reading was information overload. Most users consider the policies a nuisance and ignore them. In spite of that, various strategies for the improvement of privacy policy statements are seen as important in facing users' concerns regarding privacy [18,19].

In their study, Obar and Oeldorf-Hirsch [17] found out that people often ignore privacy and terms of service policies of social networks regardless of whether they are signing up for a new service or if the policies change. The median reading time was 13.6 s. The clickwrap allowing to bypass the policy and just to click to agree to it was used by 74% of respondents. That suggests that the implementation of clickwraps supports the ignoring behaviour. Even though the tested policies had problematic parts, 97% of participants agreed to privacy policy and 93% to the terms of service. A self-reported question on the behaviour regarding policies of big social networks has shown that over 35% of respondents ignore them. Considering the privacy paradox, the actual behaviour may differ significantly. Even the GDPR regulation does not provide a solution as it states in Section 32 that the subject's consent to processing his information may be just ticking a box and that the processes for gaining the consent must not be disruptive to the use of provided services.

Barocas and Nissenbaum [20] identified three reasons for privacy policy ineffectiveness: (1) confusing disconnect between the privacy policy of online publishers and the tracking and targeting of third parties with whom they contract and who have their own privacy policy, (2) privacy policy may change at any time just with a short notice and (3) the increasing number of players in the advertising network and exchange space that results in unclear flows of users' data. They conclude that meaningful notices are illusory. They suggest a solution based on the theory of contextual integrity [21].

Cate and Mayer-Schönberg [22] summarise the discussions during the regional privacy dialogues and the global privacy summit hosted by Microsoft in 2012. The key point is that the era of big data era and the complexity of online social interactions call for adjustments in information privacy regulations to meet the new needs. Privacy protection should be more effective and efficient. Individuals should be protected.

Bakos, Marotta-Wurgler and Trossen [19] carried out a research in 2007 involving more than 48,000 respondents and found out that terms of service policies were accessed by only 0.2% of them. The median time spent on the policy page was 30 s. A repeated similar study in 2012 showed that clickwraps have no impact on users. It should be noted in passing that the privacy paradox makes the investigation of policy behaviour more difficult as people usually say they take care of their privacy, but their actions are different. There is another reason why users ignore terms of service or privacy policies: they cannot do anything about them anyway. If the customer wants to buy at a shop, s/he can either accept the conditions or he cannot buy anything. Users' behaviour regarding privacy differs. The type of information required by the web site can be classified as contact, biographical or financial [23]. Their research has shown that users are more willing to provide contact than biographical information and least willing to provide financial information. Younger, educated and affluent users require a stronger protection than the older, less educated or poorer ones. The results, however, apart from other things show that 77.4% of the respondents had seen a privacy policy statement before the research, but only 45.6% had read it.

Privacy statements were found to increase the willingness to disclose information [24], to pay for products and services [25], to support trust [26]. However, they have also been criticised because they are long, difficult to understand and thus they are often ignored [27,28]. They are more difficult to understand than the average issue of The New York Times [29] and their complicatedness increases with time [30].

Many articles dealing with the topic of privacy statements focus on the effects of these statements on users' attitude towards companies or their services. Trust seems to be a frequent topic of many research projects. Nemati, Van Dyke [31] found that when customers read privacy statements, their trust in the company increases. Bansal et al. [9] investigated the differences between users concerning their perception of privacy assurance mechanisms including privacy statements. They confirmed the moderating role of users' privacy concerns in trust formation.

Very interesting is the article by [32] who researched the privacy expectations and privacy notices of fictitious web pages. The results show that respondents saw more protection in the notices than they really offered. They projected their privacy expectations onto the privacy notices. Second, they still considered them insufficient in meeting their private expectations. That is an important finding for the privacy statement formulation.

In our research we did not focus on the effects of privacy policy statements, but rather on the determinants of their reading, i.e., on users' privacy protecting behaviour.

3. Protective Behaviour

Users' behaviour protecting privacy belongs to the category of information security behaviour. This type of behaviour has been studied in companies and higher educational institutions [33]. Predominantly, behavioural models have been used to identify factors influencing intention towards protective behaviour and its real execution. The theory of reasoned action or its extension of the theory of planned behaviour has been used very frequently in the research of information security awareness and information security behaviour. According to the meta-analysis carried out by [33] 38% of articles dealing with information security awareness and behaviour uses these two theories. The second most used theory comprises 24%.

As we have stated, the theory of planned behaviour and its modifications are popular in this area of research and show good results in explaining users' behaviour. We combined this theory with the theory of privacy calculus to prepare a model grasping users' behaviour concerning privacy policy statements (reading them).

4. Theory of Planned Behaviour

The theory of planned behaviour (TPB) states that intentions are influenced by attitude, norms and perceived control. There is no universal ordering of the importance of these factors. The relative importance of the factors is different for different cultures and behaviours [34]. The originators of the theory of planned behaviour agree to modifications of the theory and inclusion of additional variables [35,36]. This theory has been used frequently [33] and is effective in explaining human behaviour. It is an extension of the theory of reasoned action because it supplements the theory of reasoned action with the aspect of control over the behaviour. It suggests that behavioural intentions and actual behaviour are influenced by the attitude towards the behaviour, normative pressures towards the behaviour called subjective norm and perceived behavioural control. Attitude represents the positive or negative feeling towards the behaviour (its evaluation). Attitudes are determined by consequences and outcomes of the behaviour. Behavioural control refers to the perceived difficulty of the behaviour and probability of its success. TPB has been used to explain and predict human behaviour in adopting ICTs [37–40]. Our model interlinks the TPB theory with the privacy calculus model and trust.

TPB Components

If somebody develops a positive attitude towards privacy policy statements (PPS), s/he will probably like to know them, to read them. A positive evaluation of the attitude will lead to the intention to realise the behaviour. Norms may further influence the intention to read the privacy policy statements, too. If people who are close or important to the person perform the behaviour or think the person should perform the behaviour, it is likely that the person will follow their opinion. According to [41], the subjective norm will

influence the person's intention to act accordingly. Additionally, the greater the behavioural control the greater the person's intention—in our case the intention to read the privacy policy statements—will be. We defined behavioural control as the degree of understanding the privacy policy statements including the willingness to invest time and effort into understanding them.

In Fishbein's and Ajzen's view [42] a person's attitude towards a behaviour is determined by the beliefs about the behaviour which consists in subjective probability that the behaviour will produce a certain outcome. The attitude is influenced by the outcome evaluation and the subjective probability that the behaviour produces the outcome. That is why we formulated the following hypotheses:

Hypothesis 1 (H1). *Attitudes toward PPS are positively related to the intention to read them.*

Hypothesis 2 (H2). *Subjective norms supporting reading PPS are positively related to the intention to read PPS.*

Hypothesis 3 (H3). *Perceived behavioural control (degree of understanding) is positively related to the intention to read PPS.*

Ajzen himself [43] proposes that intention is positively related to actual behaviour. Therefore, we formulate the hypothesis that

Hypothesis 4 (H4). *The intention to read PPS is positively related to users' real behaviour (reading the PPS).*

5. Privacy Calculus

Privacy protection and privacy disclosure is related to the process of boundary management. People want to achieve a specific level of privacy and consider the perceived benefits and risks [44]. The privacy calculus theory compares the risks and benefits gained [45]. Private information disclosure is the result of a rational comparison or weighting the costs and benefits of disclosure. This approach is not satisfactory for the explanation of the behaviour as it does not consider bounded rationality caused by lack of information, situational constrains or cognitive abilities. Furthermore, the empirical evidence does not unanimously support this way of thinking, there is conflicting evidence for it [46]. The inconsistencies concern especially the role of privacy concerns in privacy disclosure. The gratifications were less controversial, and they seem to support the wish to disclose especially in social networks. We will use the theory of privacy calculus to find determinants of the attitude towards reading PPS.

The effect of privacy concerns on attitude has been discussed in literature. Phelps [47] found the negative relation between consumers' attitude towards direct marketing and privacy concerns. Cases [48] also confirmed the negative influence of privacy concerns on attitude towards email campaigns. Chellapa [49] concluded that privacy concerns lead to negative attitudes about using a technology.

A similar way of reasoning can be formulated in terms of privacy disclosure benefits. Users who evaluate the benefits resulting from privacy disclosure positively will not be as concerned about their privacy and interested in privacy policy statements.

Some studies [50] found that adolescents and youths are more willing to disclose their personal data when commercial incentives are offered. The study by Youn [51] revealed that older adolescents are willing to disclose their personal information if the perceived benefits exceed the costs related to the disclosure. On the other hand, individuals that are more concerned about their online privacy are less willing to disclose their personal information. [52,53]. Based on these findings we formulated the following two hypotheses:

Hypothesis 5 (H5). *Privacy risks are negatively related to the attitude towards reading PPS.*

Hypothesis 6 (H6). *Privacy benefits are positively related to the attitude towards reading PPS.*

As for trust, it has been found that institutional trust which can be defined as the confidence that the medium requesting data will not misuse them [54] is related to privacy concerns [55], risk beliefs [56] and intentions to disclose information [10]. Some studies defined institutional trust in general terms as the degree of confidence in the internet [10] or data collecting service [57]. Trust may be understood as the confidence in the data collecting medium. Trust is a protective factor that mitigates risk beliefs and privacy concerns. We formulated the determinants of trust in such a way that it included distrust as its other extreme which may support privacy concerns.

Some studies [45,58] found a negative relationship between privacy concerns and the intention to disclose private information. However, the TPB states that additional factors have indirect influence only because their influence is mediated by attitude, subjective norm or behavioural control [59].

Trust has been studied in social sciences and management [45,60]. It can be defined with [61] as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the others will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (p. 712). This definition applies to online transactions, including online activities, too.

Trust is related to the expectation of beneficial behaviour towards the person; the person believes that the company and its technology will act in the person's interest [62,63]. When the person trusts the company and its technology, s/he will believe in the benefits of PPS and will more likely read them. Therefore, we formulated the following two hypotheses:

Hypothesis 7 (H7). *Trust is positively related to the benefits of privacy disclosure.*

Hypothesis 8 (H8). *Trust is negatively related to the risks of privacy disclosure.*

The theoretical research model can be found in Figure 1.

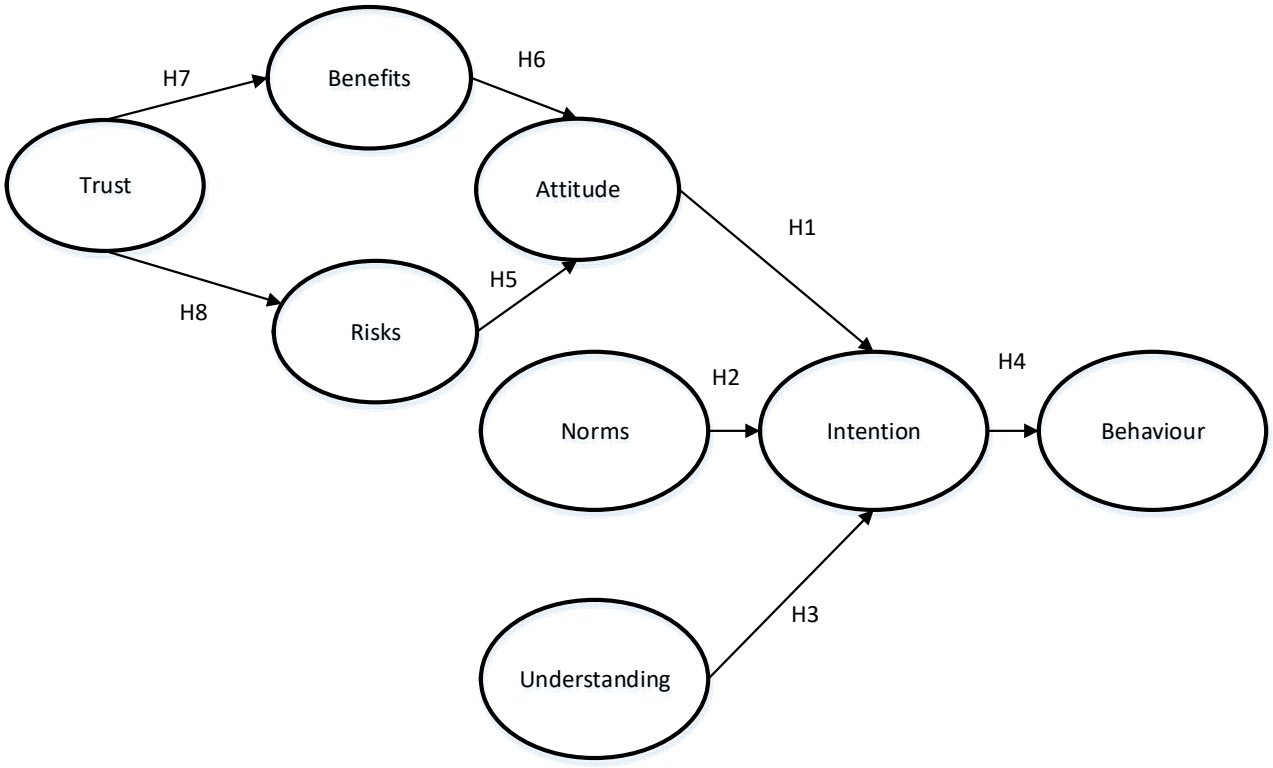

Figure 1. Research model.

6. Research

6.1. Materials and Methods

We carried out a survey of university students' behaviour in the online environment and their relationship towards privacy statements. The research used the method of questionnaire distributed online from 8nd December 2020 to 7th January 2021 through Google Forms. The respondents were university students from the Prague University of Economics and Business, Czech Republic. We focused on this target group as the author of the article is a university teacher and so he can address this target group easily. The respondents are young students studying at the Faculty of Informatics and Statistics of the Prague University of Economics and Business. They have economic background, but their field of study is applied informatics and related fields. Their generation is called Generation Z—they are digital natives, since their youth they have been exposed to the internet, social networks and mobile devices. They seem to be more idealistic, more confrontational and less accepting of diverse points of view [64]. Our respondents were university students of informatics, which means they have better IT skills and are more aware of the risks present in the online environment. They know how technologies work and what they can be used for. It would be interesting to compare the results of this research with other target groups, such as Generations X or Y. The problem is, however, the low response rate of these groups.

Young adults were selected because they have been found to be faster adopters of mobile services [65]. The selected target group allows identification of how the young generation familiar with modern technologies and acquainted with their risks perceives the privacy policy. They use technologies a lot and we should know what type of communication works best for them.

We received 163 answers to our questionnaire. The respondents were 19–26 years old. In total, 59% of them were males, 41% females. We used the 5-point Likert scale in the answers with 1 meaning "definitely no" and 5 "definitely yes". We applied the partial least square method to quantify the influence of individual factors. For the results calculation, the program Smart PLS v3 was used. We used partial least squares (PLS) component-based structural equation modelling because of the explicatory focus, testing of interaction terms of latent variables, sample size and number of paths (e.g., [66–68]. We used a bootstrap of 500 resamples to assess the parameter estimate significance because partial least squares regression is a distribution-free technique (e.g., [69]). Due to the smaller sample size and number of latent variables and paths, the standard SEM was not suitable. Wold [68] refers to the partial least square method as a soft modelling approach because it does not require restrictive assumptions prevalent to other methods of latent variable path analysis. [70] mentions only that for the partial least square method Xs need not be independent, the system is a function of a few underlying latent variables, the system should exhibit homogeneity throughout the analytical process, and the measurement error in X is acceptable.

The model was evaluated as follows: the individual item reliability of measurement model is measured by Cronbach's alpha. Table 1 presents the factors and their items and Table 2 shows that Cronbach's alpha values of all constructs are above 0.7 which is acceptable as the Cronbach's alpha coefficients should be greater than or equal to 0.7 [71,72]. In this respect, we can accept that all constructs are reliable. Additionally, average variance extracted values greater than 0.5 suggest that the measurement model has adequate convergent validity [73]. The square root of the average variance extracted should be higher than any of the correlations between each latent variable to assess discriminant validity [71]. In Table 3, values on the diagonal of the table show the average variance extracted values for each latent variable, and these values are higher than any of the values above or below them in the same column. It implies that the measurement model has discriminant validity.

Table 1. Factors and items.

Code	Factors
	Trust
T1	I would allow an online service to influence an important issue
T2	I would allow an online service to influence my future
T3	I would like to control the functioning of online services
T4	I would let an online service decide an important problem
	Privacy disclosure risks
R1	I fear that online services store my personal data
R2	I fear that the policies against errors in private data do not work sufficiently
R3	I fear that my online personal data are used for other purposes than stated
R4	I fear that my online personal data are accessible to unauthorised persons
R5	I fear that by combining various personal data new facts can be revealed
R6	I fear that the automatic functioning of online services may lead to decisions harmful to privacy
	Privacy disclosure benefits
B1	I welcome cheaper products and services (discounts) in exchange for private information
B2	I welcome personalised services in exchange for private information
B3	I welcome higher popularity in exchange for private information
B4	I welcome more relevant offers and proposals in exchange for private information
	Attitude towards reading the privacy policy statements
AT1	Reading privacy statements is unfavourable—favourable
AT2	Reading privacy statements is useless—useful
AT3	Reading privacy statements is a bad idea—good idea
AT4	Reading privacy statements is unimportant—important
AT5	Reading privacy statements is unnecessary—necessary
	Subjective norms
NORM1	People who are important to me think I should read the privacy statements
NORM2	People who are important to me would approve of my reading privacy policy statements
NORM3	People who are important to me read privacy statements
NORM4	The rules of online behaviour that I follow say I should read the privacy policy of online services
	Understanding the privacy policy statements
UND1	I understand the privacy policy statements
UND2	I am well informed on the privacy policy statements
UND3	I am ready to invest time into understanding the privacy policy statements
UND4	I am ready to invest effort into understanding the privacy policy statements
Intention to read privacy policy statements	
INT1	I plan to read the PPS (privacy policy statements)
INT2	I would like to read the PPS
INT3	I am resolved to read the PPS
BEH	I read the privacy policy statements

Table 2. Factors, items and their characteristics.

Code	Mean	SD	Cronbach's Alpha
Trust			0.882
T1	2.44	1.2	
T2	2.67	1.66	
T3	2.26	1.34	
T4	2.07	1.09	
Risks			0.895
R1	3.91	1.16	
R2	3.74	1.03	
R3	3.71	1.00	
R4	3.61	1.21	
R5	3.37	1.27	
R6	3.39	1.35	
Benefits			0.869
B1	2.23	1.3	
B2	1.98	1.2	
B3	1.75	0.96	
B4	2.26	1..34	
Attitude			0.882
AT1	3.43	1.27	
AT2	3.86	1.22	
AT3	4.07	1.16	
AT4	3.95	1.3	
AT5	3.94	1.27	
Norms			0..79
NORM1	2..93	0..87	
NORM2	3.61	1.02	
NORM3	2.28	0.78	
NORM4	3.74	0.96	
Understanding			0.825
UND1	2.98	1.07	
UND2	2.82	0.99	
UND3	2.16	1.13	
UND4	1.67	1.16	
Intention			0.785
INT1	3.04	0.92	
INT2	3.56	1.41	
INT3	2.81	1.12	
Behaviour			
BEH	2.76	1.24	

Table 3. AVE (diagonal) and latent variables correlations.

	Trust	Risks	Benefits	Attitude	Norms	Understanding	Intention	Behaviour
Trust	0.693							
Risks	−0.387	0.655						
Benefits	0.362	−0.079	0.715					
Attitude	−0.385	0.629	−0.418	0.68				
Norms	−0.354	0.213	−0.034	0.34	0.605			
Understanding	−0.059	0.127	0.072	0.153	0.169	0.656		
Intention	−0.507	0.359	−0.124	0.451	0.579	0.602	0.699	
Behaviour	−0.429	0.274	−0.039	0.253	0.455	0.297	0.622	1

The responses are based on self-evaluation of the respondents which may be the source of bias. The sample consists of university students studying economics and applied IT, which is a further limit of this study. However, the questionnaire did not require any expert knowledge and so the results can to some extent be generalised for the whole young Generation Z. Another limitation of the research consists in the fact that there may be other influences or factors not included in the behavioural theories used.

We used a 5-point Likert scale (ranging from 1—definitely no to 5—definitely yes) to measure the factors. Privacy concern was measured using a scale with six dimensions of privacy risks (collection, unauthorised use, improper access, errors, reduced judgment, and combining data) suggested by [74]. For the measurement of trust a 4-item trust scale adapted from [75] was used with the items trust in technology in important issues, accepting its influence on the person's future, controlling its functioning, and trust in its decision of serious problems. For the measurement of attitude, the 5-point scale adapted from [76] was used, for the measurement of social norm their 3-point scale and for the measurement of the intention their 3-point scale was adapted. To measure the behavioural control, we used the latent variable of understanding consisting of understanding the PPS, orientation in them, time and effort necessary for understanding. For the real behaviour we used only one variable.

The questionnaire was validated on two students and two academic employees. They expressed a good understanding of the questions. The members of the academic staff also understood the latent factors. All respondents had the option to comment on the questionnaire and they did not express any doubt or confusion concerning the questionnaire.

6.2. Results

We used eight categories of questions: trust in technologies, privacy disclosure risks, privacy disclosure benefits, attitude towards reading privacy statements of online services, subjective norms related to reading privacy statements, understanding of privacy statements and related problems, intention to read the statements, and real reading of the statements. The factors and their items are depicted in Table 1.

As for the path coefficients, all of them were significant at the 5% significance level. The path coefficient between trust and risks was −0.387; between trust and benefits it was 0.362; between risks and attitude it was 0.6; between benefits and attitude the path coefficient was −0.371; between attitude and intention it was 0.233; between norms and intention it was 0.416; between understanding and intention it was 0.495; between intention and behaviour it was 0.622. That means all hypotheses were confirmed. The R^2 (amount of variance explained by the model) of benefits achieved 0.131; R^2 of risks 0.149; R^2 of attitude 0.533; R^2 of intention 0.644; R^2 of behaviour 0.387.

7. Discussion

All outlined hypotheses were confirmed at the 5% significance level as can be seen in Figure 2.

Figure 2. Path coefficients of the research model.

The standard deviations of the answers to our questions are within the context of similar studies; e.g., [77,78] have similar standard deviations in their studies. The theory of planned behaviour is a standard behavioural theory and its factors were confirmed by many studies.

Our model confirms that trust influences both the perceived benefits (H7) and risks (H8) related to privacy. Benefits are the more welcome and risks are the less feared the more the person trusts online services. The strength of the influence is similar with regard to benefits and risks. The effect of trust on privacy concerns and disclosure has been confirmed e.g., by [55,58].

Both benefits and risks influence the attitude towards reading PPS, benefits negatively (H6), risks positively (H5). [47,48] came to similar conclusions in their studies of privacy risks. [50,51] found out that benefits affect privacy concerns of youths. The influence of risks is stronger in our study. If the person fears the risks of the online environment, s/he will consider reading the PPS more important. It shows that fear has a stronger effect on attitude towards PPS than benefits.

In accordance with the theory of planned behaviour, we can differentiate three antecedents of the intention: attitude, norms and control. The strengths of these factors differentiate according to the context, but usually the attitude has the strongest influence [33]. Our study has a specific context where the control factor, i.e., intricacy, vagueness and complexity of the PPS has the strongest effect on the intention to read the PPS (H3). As the PPS are difficult to read and respondents do not understand them, they do not want to read them. They are, however, influenced by others or by social norms to read them (H2). Their positive attitude towards reading them affects the intention to read,

too, but weaker than problems with their understanding or social pressure (H1). The upshot is that the complexity of PPS is a substantial obstacle to the intention to read them. Even if the respondent has a positive attitude towards reading the PPS, the problems with understanding block their intention. What should be done is to support students' positive attitude towards reading the PPS, solve the problems related to the understanding of PPS and keep supporting the social norms.

The intention to read the PPS is not fully projected into the actual behaviour (H4), but that is a common issue in the theory of planned behaviour. The reasons are not fully clear, but there are many obstacles that lie between the intention and realisation, such as lack of time, lack of motivation, lack of energy etc. The difference between intention and action is a typical issue, see e.g., [79]. In our model, the factor of behaviour had one item only, which adds another reason for the difference between intention and real behaviour.

In our research, the answers concerning reading the privacy statement showed a low level of reading them, the mean was below the middle of the Likert scale, the intention to read them was somewhat higher—around the middle of the Likert scale. We found that understanding the PPS and subjective norms have the strongest influence on reading the PPS. The influence of attitude is also significant, but not as strong. That indicates that for young people the PPS are not important with regard to their privacy, they do not trust them. Young people are more influenced by others and by the difficult understanding of PPS; the normative pressure of others and the positive experience with understanding the PPS together with the willingness to invest time and effort are stronger determinants. Young people are in general more socially oriented as their personality is not yet fully developed [80]. Today's society is oriented on entertainment, amusement [81,82] and easy availability of things and that is why the willingness to overcome the difficulties related to reading the PPS is weak. Another reason lies in the fact that the PPS are not transparent and well formulated. A further research would be necessary to distinguish the strength of these two individual factors.

Trust affects both risks and benefits and those in turn have an effect on the attitude towards reading the PPS. Risks haves a stronger influence on the attitude. That is logical as the PPS are supposed to protect privacy and eliminate the fears of privacy risks.

The reasons for the ineffective functioning of privacy notices and controls were analysed by [83]. It seems that users share personal data voluntarily as they extensively use many applications that collect their personal data, construct users' profiles and purchasing styles, the data are analysed, combined with other data and used for targeted advertising. The modern wearables are a recent invention that collects a lot of data. With the advent of the Internet of Things, privacy will be threatened even more. These devices are very popular and widely used and the PPS are heterogenous, complicated and tricky.

The fact that many users take advantage of technologies that invade their privacy and do not care about the privacy policies does not mean individuals surrender privacy, but that they feel helpless, lost and confused [43,84]. The intrusions into privacy are often hidden and users do not know that their private data has been collected and processed, not to mention the fact that they cannot predict how and when their information will be used. Users do not understand what data are used and how because such an understanding would require both technical and sociological expertise.

Schaub, Balabako' and Cranor's idea [83] is to make privacy notices useful, usable and unobtrusive. They suggest the privacy notice to be (1) relevant in the current transactional context, (2) actionable, i.e., the user's choice and consent should be specific and explicit and (3) understandable, easy to use and not overloading with information. To realise these principles, Schaub, Balabako and Cranor [83] recommend: (1) differentiating privacy policies according to various users (primary, secondary, incidental, protected); (2) provision of short and specific privacy notices adapted to specific context, system feature and audience; (3) highlighting unexpected and context violating practices with details on demand; (4) leveraging the notice by appropriate timing, channel (primary, secondary for e.g., fitness tracker or public in e.g., public spaces), modality (visual, auditory, haptic) and

control (blocking, non-blocking, decoupled). Considering what has been said above, it is questionable if these measures will secure effective privacy notices. Additionally, we must not forget the complexity and intricacy of today's IT world which does not allow for easy explanation of the practices and technical subtleties. Either the matter is too complicated, or nobody can anticipate all details and directions where the data processing may lead. Privacy is an issue where the complexity and functioning of the world surpasses human ability to make a sense of it.

The situation will not have a simple solution. A hint towards one would be if companies started to respect users, understand their expectations and come to realise that what they do is not only profit oriented, but that it also should make sense. Another one, to which our model may also hint dwells in the death of the subject. One's identity will be defined by others and by the activity performed or product used, similar to the postmodern consumer, postmodern marketing and Baudrillard's hyperreality.

8. Contributions and Implications

This study combined the privacy calculus theory and the theory of planned behaviour to explain the attention paid to privacy policy statements. The lack of understanding of PPS is considered the most significant problem and hinders the effects of transparency. In previous studies, the effects of PPS were investigated, but not the intention to read them by users. This approach makes our contribution unique. The combination of theory of planned behaviour and the privacy calculus is also new.

The practical implications for policy makers, for organisations and service providers consist in the support of positive attitude towards PPS, in the information and media literacy that would explain the intricacies of PPS and in the effort to respect the expectations of users concerning their privacy even in the service design.

9. Limitations and Future Research

Privacy policy statements are important tools in the privacy boundary management [85]. However, we have to consider the context-specific nature of our results. The specificity of users and contexts was not considered in our research. Our research is also limited by the country where it was carried out. Some studies [12,86] contend that the standards of policy implementation and enforcement have an effect on people's attitude towards PPS. More studies from various countries with varying levels of privacy policy implementation and enforcement should be performed. Other demographic variables and IT specific skills should be also considered to get more accurate results.

Future studies should concentrate on various contexts, e.g., banks, SNS, e-commerce to draw a more colourful picture of the situation. They should also consider other demographic and personal features and skills to differentiate between different segments.

10. Conclusions

To conclude, we may say that even though privacy policy statements attempt to decrease the information asymmetry, they collide with the users' inability to achieve symmetry. They are too complex, vague and complicated and users do not want to read them. They can be motivated by other opinion makers to read them, but their own attitude towards reading the PPS is weaker than the problems with understanding. A similar situation can be found in other examples of transparency which is often related to information overload. The world is becoming too complex and complicated and people are not able to understand all information necessary for their orientation and decision-making. The cybernetic law of requisite variety formulates it, too. Man is a rational being. Our research has confirmed the rationality of man in the privacy calculus. Trust influences the perception of risks and benefits and they influence the attitude.

The problem as has been demonstrated on the example of privacy statements is not just the excess of information, but also the working of technologies that is not translatable into human categories. The technologies may use values that are not acceptable for humans and

the processes they use in their decision-making (especially in the case of neural networks) cannot be explained in human categories. The problem is currently most pressing in the area of privacy, but with the implementation and use of technologies in all areas of human life, the consequences will become more serious. The human world will start to resemble the absurd world of Franz Kafka's stories and its inhabitants will have similar feelings to the characters of existential novels where the system is more powerful than the individual. How man will react remains an open question.

Funding: This paper was processed with a contribution from the University of Economics in Prague, IG Agency, OP VVV IGA/A, CZ.02.2.69/0.0/0.0/19_073/0016936, grant number F4/05/2021.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The paper was carried out with the financial support of IGA/A GC, OP RDE IGA/A, CZ.02.2.69/0.0/0.0/19_073/0016936 and IGA F4/5/2021, ES409050 Social Ties and Interactions in Online Environment.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Culnan, M.J. Policy to avoid a privacy disaster. *J. Assoc. Inf. Syst.* **2019**, *20*. [CrossRef]
2. Janssen, M.; van der Voort, H.; Wahyudi, A. Factors influencing big data decision-making quality. *J. Bus. Res.* **2017**, *70*, 338–345. [CrossRef]
3. Erevelles, S.; Fukawa, N.; Swayne, L. Big data consumer analytics and the transformation of marketing. *J. Bus. Res.* **2016**, *69*, 897–904. [CrossRef]
4. Janssen, M.; van den Hoven, J. Big and open linked data (BOLD) in government: A challenge to transparency and privacy? *Gov. Inf. Q.* **2015**, *32*, 363–368. [CrossRef]
5. TRUSTe Smart Privacy for Smartphones: Understanding and Delivering the Protection Consumers Want. 2011. Available online: www.truste.com (accessed on 24 March 2021).
6. Janssen, M.; Kuk, G. The challenges and limits of big data algorithms in technocratic governance. *Gov. Inf. Q.* **2016**, *33*, 371–377. [CrossRef]
7. Morey, T.; Forbath, T.; Schoop, A. Customer data: Designing for transparency and trust. *Harv. Bus. Rev.* **2015**, *93*, 96–105.
8. Drinkwater, D. Does a Data Breach Really affect Your Firm's Reputation. Available online: http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-reallyaffect-your-firm-s-reputation.html2016 (accessed on 24 March 2021).
9. Bansal, G.; 'Mariam' Zahedi, F.; Gefen, D. The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern. *Eur. J. Inf. Syst.* **2015**, *24*, 624–644. [CrossRef]
10. Dinev, T.; Hart, P. An extended privacy calculus model for e-commerce transactions. *Inf. Syst. Res.* **2006**, *17*, 61–80. [CrossRef]
11. Joinson, A.N.; Reips, U.-D.; Buchanan, T.; Schofield, C.B.P. Privacy, trust, and self-disclosure online. *Hum.-Comput. Interact.* **2010**, *25*, 1–24. [CrossRef]
12. Xu, H.; Dinev, T.; Smith, J.; Hart, P. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *J. Assoc. Inf. Syst.* **2011**, *12*, 798–824. [CrossRef]
13. Chua, H.N.; Herbland, A.; Wong, S.F.; Chang, Y. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telemat. Inform.* **2017**, *34*, 157–170. [CrossRef]
14. Liu, C.; Arnett, K. An examination of privacy policies in Fortune 500 Web sites. *Mid-Am. J. Bus.* **2002**, *17*, 13–22. [CrossRef]
15. Cate, F.H. The failure of fair information practice principles. In *Consumer Protection in the Age of the Information Economy*; Winn, J.K., Ed.; Ashgate Publishing: Surrey, UK, 2006; pp. 343–379.
16. Adler, R.S. The last best argument for eliminating reliance from express warranties: "Real-world" consumers don't read warranties. *South Carol. Law Rev.* **1994**, *45*, 429.
17. Obar, J.A.; Oeldorf, H.A. The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Inf. Commun. Soc.* **2018**, *23*, 128–147. [CrossRef]
18. Federal Trade Commission. Protecting Consumer Privacy in an Era of Rapid Change. Federal Trade Commission Report. 2012. Available online: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (accessed on 24 March 2021).
19. Bakos, Y.; Marotta-Wurgler, F.; Trossen, D.R. Does anyone read the fine print? Consumer attention to standard-form contracts. *J. Leg. Stud.* **2014**, *43*, 1–35. [CrossRef]

20. Barocas, S.; Nissenbaum, H.F. On Notice: The Trouble with Notice and Consent. Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information. Available online: https://ssrn.com/abstract=2567409 (accessed on 24 March 2021).
21. Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*; Bibliovault OAI Repository, the University of Chicago Press: Chicago, IL, USA, 2010.
22. Cate, F.H.; Mayer-Schönberger, V. Notice and consent in a world of Big Data. *Int. Data Priv. Law* **2013**, *3*, 67–73. [CrossRef]
23. Meinert, D.; Peterson, D.; Criswell, J.; Crossland, M. Privacy policy statements and consumer willingness to provide personal information. *JECO* **2006**, *4*, 1–17. [CrossRef]
24. Phelps, J.; Glen, N.; Elizabeth, F. Privacy Concerns and Consumer Willingness to Provide Personal Information. *J. Public Policy Mark.* **2000**, *19*, 27–41. [CrossRef]
25. Tsai, J.Y.; Serge, E.; Lorrie, C.; Alessandro, A. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Inf. Syst. Res.* **2011**, *22*, 254–268. [CrossRef]
26. Tang, Z.; Hu, Y.J.; Michael, D.S. Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *J. Manag. Inf. Syst.* **2008**, *24*, 153–173. [CrossRef]
27. Calo, R. Against Notice Skepticism in Privacy (and Elsewhere). *Notre Dame Law Rev.* **2012**, *87*, 1027–1072.
28. Martin, K. Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online. *First Monday* **2013**, *18*. Available online: http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802 (accessed on 11 August 2020). [CrossRef]
29. Sheehan, K.B. In Poor Health: An Assessment of Privacy Policies at Direct-to-Consumer Web Sites. *J. Public Policy Mark.* **2005**, *24*, 273–283. [CrossRef]
30. Milner, C.; Culnan, M.J.; Greene, H. Longitudinal Assessment of Online Privacy Notice Readability. *J. Public Policy Mark.* **2006**, *25*, 238–249. [CrossRef]
31. Nemati, H.R.; Van Dyke, T.P. Do Privacy Statements Really Work? The Effect of Privacy Statements and Fair Information Practices on Trust and Perceived Risk in E-Commerce. *Int. J. Inf. Secur. Priv.* **2009**, *3*, 45–64. [CrossRef]
32. Martin, K. Privacy Notices as Tabula Rasa: An Empirical Investigation into how Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online. *J. Public Policy Mark.* **2015**, *34*, 210–227. [CrossRef]
33. Lebek, B.; Uffen, J.; Neumann, M.; Hohler, B.H.; Breitner, M. Information security awareness and behavior: A theory-based literature review. *Manag. Res. Rev.* **2014**, *37*, 1049–1092. [CrossRef]
34. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Processes.* **1991**, *50*, 179–211. [CrossRef]
35. Ajzen, I. The theory of planned behavior: Reactions and reflections. *Psychol. Health* **2011**, *26*, 1113–1127. [CrossRef] [PubMed]
36. Fishbein, M.; Ajzen, I. *Predicting and Changing Behavior: The Reasoned Action*; Taylor & Francis: Abingdon, UK, 2010.
37. Carter, S.; Yeo, A.C.-M. Mobile apps usage by Malaysian business undergraduates and postgraduates: Implications for consumer behaviour theory and marketing practice. *Int. Res.* **2016**, *26*, 733–757. [CrossRef]
38. Cheung, M.F.Y.; To, W.M. Service co–creation in social media: An extension of 649 the theory of planned behavior. *Computers Hum. Behav.* **2016**, *65*, 260–266. [CrossRef]
39. Jiang, C.; Zhao, W.; Sun, X.; Zhang, K.; Zheng, R.; Qu, W. The effects of the self and social identity on the intention to microblog: An extension of the theory of planned behavior. *Comput. Human Behav.* **2016**, *64*, 754–759. [CrossRef]
40. Kim, E.; Lee, J.A.; Sung, Y.; Choi, S.M. Predicting selfie-posting behavior on social networking sites: An extension of theory of planned behavior. *Comput. Human Behav.* **2016**, *62*, 116–123. [CrossRef]
41. Li, M.; Dong, Z.Y.; Chen, X. Factors influencing consumption experience of mobile commerce: A study from experiential view. *Internet Res.* **2012**, *22*, 120–141. [CrossRef]
42. Fishbein, M.; Ajzen, I. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*; Addison-Wesley: Boston, MA, USA, 1975.
43. Masur, P.K.; Scharkow, M. Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Soc. Media. Soc.* **2016**, 2. [CrossRef]
44. Culnan, M.J.; Armstrong, P.K. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organ. Sci.* **1999**, *1*, 104–115. [CrossRef]
45. Trepte, S.; Reinecke, L.; Ellison, N.B.; Quiring, O.; Yao, M.Z.; Ziegele, M. A Cross-Cultural Perspective on the Privacy Calculus. *Soc. Media Soc.* **2017**, *3*, 1. [CrossRef]
46. Phelps, J.; D'Souza, G.; Nowak, G. Antecedents and consequences of consumer privacy concerns: An empirical investigation. *J. Interact. Mark.* **2001**, *15*, 2–17. [CrossRef]
47. Cases, A.; Fournier, C.; Dubois, P.; Tanner, J., Jr. Web site spill over to e-mail campaigns: The role of privacy, trust and shoppers attitudes. *J. Bus. Res.*, **2010**, *63*, 993–999. [CrossRef]
48. Chellappa, R.K.; Sin, R.G. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Inf. Technol. Manag.* **2005**, *6*, 181–202. [CrossRef]
49. Turow, J.; Nir, L. *The Internet and the Family 2000: The View from Parents, the View from Kids*; The Annenberg Public Policy Center: Philadelphia, PA, USA, 2000.
50. Youn, S. Teenagers' perception of online privacy and coping behaviors: A risk-benefit appraisal approach. *J. Broadcast. Electron. Media* **2005**, *1*, 86–110. [CrossRef]

51. Hsu, M.-H.; Kuo, F.-Y. The effect of organization-based self-esteem and deindividuation in protecting personal information privacy. *J. Bus. Ethics* **2003**, *4*, 305–320. [CrossRef]
52. LaRose, R.; Rifon, N.J. Promoting I-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behaviour. *J. Consum. Aff.* **2007**, *1*, 127–149. [CrossRef]
53. Anderson, C.L.; Agarwal, R. The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Inf. Syst. Res.* **2011**, *22*, 469–490. [CrossRef]
54. Bansal, G.; Zahedi, F.; Gefen, D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decis. Support Syst.* **2010**, *49*, 138–150. [CrossRef]
55. Malhotra, N.K.; Kim, S.S.; Agarwal, J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Inf. Syst. Res.* **2004**, *15*, 336–355. [CrossRef]
56. Krasnova, H.; Veltri, N.F.; Gunther, O. Self-disclosure and privacy calculus on social networking sites: The role of culture. *Bus. Inf. Syst. Eng.* **2012**, *4*, 127–135. [CrossRef]
57. Dinev, T.; Hart, P. Privacy concerns and levels of information exchange: An empirical investigation of intended e-services. *E–Serv. J.* **2006**, *3*, 25–59. [CrossRef]
58. Davis, F.D.; Bagozzi, R.P.; Warshaw, P.R. User acceptance of computer technology: A comparison of two theoretical models. *Manag. Sci.* **1989**, *8*, 982–1003. [CrossRef]
59. Butler, J.K. Toward understanding and measuring the conditions of trust: Evolution of the conditions of trust inventory. *J. Manag.* **1991**, *17*, 643–663. [CrossRef]
60. Mayer, R.C.; Davis, J.H.; Schoorman, F.D. An integrative model of organizational trust. *Acad. Manag. Rev.* **1995**, *20*, 709–734. [CrossRef]
61. Doney, P.M.; Cannon, J.P. An examination of the nature of trust in buyer-seller relationships. *J. Mark.* **1997**, *61*, 35–51.
62. Flavian, C.; Guinaliu, M. Consumer trust, perceived security, and privacy policy: Three basic elements of loyalty to a website. *Ind. Manag. Data Syst.* **2006**, *106*, 601–620. [CrossRef]
63. McKinsey Company. TrueGen: Generation Z and Its Implications for Companies. Available online: https://www.mckinsey.de/~{}/media/McKinsey/Industries/Consumer%20Packaged%20Goods/Our%20Insights/True%20Gen%20Generation%20Z%20and%20its%20implications%20for%20companies/Generation-Z-and-its-implication-for-companies.pdf (accessed on 8 March 2021).
64. Harris, P.; Rettie, R.; Cheung, C.K. Adoption and usage of m-commerce: A cross-696 cultural comparison of Hong Kong and the United Kingdom. *J. Electron. Commer. Res.* **2005**, *6*, 210–224.
65. Chin, W.W.; Marcolin, B.L.; Newsted, P.R. A partial least squares latent variable modeling approach for measuring interaction effects: Results from a monte carlo simulation study and an electronic–mail emotion/adoption study. *Inf. Syst. Res.* **2003**, *14*, 189–217. [CrossRef]
66. Hansen, J.M.; Levin, M.A. The effect of apathetic motivation on employees' intentions to use social media for businesses. *J. Bus. Res.* **2016**, *69*, 6058–6066. [CrossRef]
67. Wold, H.O. Soft modeling: The basic design and some extensions. In *Systems under Indirect Observations, Part II*; Wold, H.O., Jöreskog, K.G., Eds.; Elsevier Science Ltd.: Amsterdam, The Netherlands, 1982; pp. 1–54.
68. Henseler, J.; Ringle, C.M.; Sinkovics, R.R. The use of partial least squares path modelling in international marketing. In *Advances in International Marketing*; Sinkovics, R.R., Ghauri, P.N., Eds.; Emerald: Bingley, UK, 2009; pp. 277–319.
69. Wold, S.; Sjostrom, M.; Eriksson, L. PLS-regression: A basic tool of chemometrics. *Chemom. Intell. Lab. Syst.* **2001**, *58*, 109–130. [CrossRef]
70. Fornell, C.; Larcker, D. A Second Generation of Multivariate Analysis: Classification of Methods and Implications for Marketing Research. *Rev. Mark.* **1987**, *1*, 407–450.
71. Nunnally, J.C.; Ira, H.B. The Assessment of Reliability. *Psychom. Theory* **1994**, *3*, 248–292.
72. Hair, J.; Black, W.; Babin, B.; Anderson, R. Multivariate Data Analysis: A Global Perspective. *Pearson* **2010**.
73. Smith, J.H.; Milberg, S.J.; Burke, S.J. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Q.* **1996**, *2*, 167–196. [CrossRef]
74. Mayer, R.C.; Davis, J.H. The effect of the performance appraisal system on trust for management. *J. Appl. Psychol.* **1999**, *1*, 123–136. [CrossRef]
75. Heirman, W.; Walrave, M. Ponnet Predicting Adolescents' Disclosure of Personal Information in Exchange for Commercial Incentives: An Application of an Extended Theory of Planned Behavior. *Cyberpsychol. Beha. Soc. Netw.* **2013**, *16*, 81–87. [CrossRef]
76. Saeri, A.K.; Ogilvie, C.; La Macchia, S.T.; Smith, J.R.; Louis, W.R. Predicting Facebook Users' Online Privacy Protection: Risk, Trust, Norm Focus Theory, and the Theory of Planned Behavior. *J. Soc. Psychol.* **2014**, *154*, 52–369. [CrossRef] [PubMed]
77. Wang, E.S.T. Effects of Brand Awareness and Social Norms on User-Perceived Cyber Privacy Risk. *Int. J. Electron. Commer.* **2019**, *23*, 272–293. [CrossRef]
78. Hassan, L.M.; Shiu, E.; Shaw, D. Who Says There is an Intention–Behaviour Gap? Assessing the Empirical Evidence of an Intention–Behaviour Gap in Ethical Consumption. *J. Bus. Ethics* **2016**, *136*, 219–236. [CrossRef]
79. Ling, R.; Yttri, B. Hyper-coordination via mobile phone in Norway. In *Perpetual Contact*; Katz, J.E., Aakhus, M., Eds.; Cambridge University Press: New York, NY, USA, 2002.

80. Postman, N. *Amusing Ourselves to Death: Public Discourse in the Age of Show Business*; Penguin: London, UK, 1985; ISBN 0-670-80454-1.
81. Shrum. *The Psychology of Entertainment Media: Blurring the Lines between Entertainment and Persuasion*; Routledge: Abingdon, UK, 2012.
82. Schaub, F.; Balebako, R.; Cranor, L.F. Designing effective privacy notices and controls. *IEEE Int. Comput.* **2017**, *21*, 70–77. [CrossRef]
83. Turow, J.; Hennessy, M.; Draper, N. *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation*; Tech. Rep.; Annenberg School for Communication, University of Pennsylvania: Philadelphia, PA, USA, 2015.
84. Acquisti, A.; Brandimarte, L.; Loewenstein, G. Privacy and human behavior in the age of information. *Science* **2015**, *347*, 509–514. [CrossRef] [PubMed]
85. Metzger, M.J. Communication privacy management in electronic commerce. *J. Comput.-Mediat. Commun.* **2007**, *12*, 335–361. [CrossRef]
86. Harding, W.T.; Reed, A.J.; Gray, R.L. Cookies and Web Bugs: What They are and How They Work Together. *Inf. Syst. Manag.* **2001**, *18*, 17–24. [CrossRef]