

## Article

# Conceptual Research Framework of Consumer Resilience to Privacy Violation Online

Jelena Budak \*, Edo Rajh, Sunčana Slijepčević and Bruno Škrinjaric 

The Institute of Economics, Zagreb, 10000 Zagreb, Croatia; erajh@eizg.hr (E.R.); sslijepcevic@eizg.hr (S.S.); bskrinjaric@eizg.hr (B.Š.)

\* Correspondence: jbudak@eizg.hr; Tel.: +385-1-236-2228

**Abstract:** This is a conceptual paper that aims to identify relevant approaches for assessing consumer resilience with regard to online privacy violation and to develop a research model suitable for subsequent empirical testing. Based on the relevant literature, we made a synthesis of theoretical approaches to individual resilience from diverse disciplines and in the next step we proposed a set of variables in the model to serve as determinants and behavioral consequences of consumer resilience with regard to online privacy violation. Finally, we offer the developed conceptual model for further scholarly debate and for future empirical verification from the research community.

**Keywords:** resilience; consumer behavior; online privacy; conceptual research model



**Citation:** Budak, J.; Rajh, E.; Slijepčević, S.; Škrinjaric, B. Conceptual Research Framework of Consumer Resilience to Privacy Violation Online. *Sustainability* **2021**, *13*, 1238. <https://doi.org/10.3390/su13031238>

Academic Editor: Marc A. Rosen  
Evangelos Grigoroudis  
Received: 27 November 2020  
Accepted: 21 January 2021  
Published: 25 January 2021

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



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Although resilience and privacy have been explored from many angles in different research fields, a debate on resilience concepts and definitions continues and the theoretical approaches needed to underpin empirical studies of resilience to privacy violation are lacking. This is particularly true given the scarce literature on consumer resilience [1] and the lack of empirical studies on consumer resilience with regard to online privacy violation.

This work represents a step forward in conceptualizing the research model to assess consumer resilience with regard to online privacy intrusion. This paper combines consumer behavior theories with resilience theories, given that resilience is a multifaceted concept requiring a holistic approach. It aims to fill the aforementioned gap and to trace the research path to explore how consumers react to the violation of their privacy online and the behavioral consequences of that stressful event. In this paper, privacy breaches are considered from the perspective of an individual's subjective assessment, meaning when an individual Internet user feels that his or her privacy has been violated. This contrasts with the “engineering” point of view of a privacy breach in which, for example, a system administrator notices an intrusion in a system's network. To assess this research issue, this conceptual paper develops a research model of consumer resilience to online privacy violation. The proposed model is open to be empirically tested to investigate the capacity of individuals to rebound from adversity, depending on subjects' individual, and other socioeconomic characteristics. Moreover, it is important to note that, although consumers might subjectively experience violation of their privacy in online environment, there are various technological solutions that can decrease and mitigate such privacy breaches [2–4].

There are four aims of this conceptual paper: (i) firstly, it provides a brief contemporary review of resilience-related concepts, focusing on social research domain with strong emphasis on individual consumer's behavior; (ii) next, this paper presents a conceptual model of consumer resilience to privacy violation in an online environment; (iii) thirdly, this paper suggests a list of variables to be used in designing such a model, as well as their theoretical justification for including them in the model; and (iv) finally, this paper provides a summary of proposed guidelines for the future model's empirical validation.

This conceptual paper is a valuable addition to the existing literature in several ways. Firstly, given the increasing digitalization rate of entire global value chain due to recent breakthroughs in modern technology, there is an increasing need for (individual) information to be available online. Although both the individual and the whole society have certain advantages by “going digital”, the flip side of the coin is an increased possibility of online privacy intrusion. Hence, a growing attention is given to factors that would make an individual more resilient to adverse effects of these online privacy violations, both by academic and professional communities. Secondly, ever since the introduction of General Data Protection Regulation (GDPR), online security and privacy have gained importance both in companies’ policies and in public discourse. Thirdly, the conceptual research framework presented in this paper is a novelty since it explores consumers’ resilience to the violation of their privacy online. This is particularly important given that neither the “resilience” nor the “privacy” concept originated within the social domain or the online environment, and to the best of our knowledge, this is the first attempt to reconcile these two concepts from a consumer-based perspective. Finally, the conceptual model proposed in this paper, together with extensive list of variables and their justification for inclusion on the model, can be considered as a handbook for future empirical validation of such a model.

The paper proceeds with descriptions of a non-systematic method of a literature review. Different theoretical concepts of resilience that might be borrowed and adapted from different disciplines to the research of individual consumer resilience to online privacy violation are presented in Section 3. In Section 4, a conceptual model of consumer resilience to online privacy violation is described, and the list of variables proposed and elaborated. The final section provides a summary of the model developed and presents guidelines for its future empirical validation.

## 2. Methodology

We applied a non-systematic literature review method in our research. The main goal of the non-systematic literature review method was to identify a gap in the literature and to define future research directions [5–8]. These goals were in compliance with our paper’s main purpose to develop the future research framework for assessing consumer resilience to online privacy violation. A flow chart of the entire process of the literature search is depicted in Figure 1. Literature searches were conducted through several iterations in Google Scholar database using relevant keywords related to resilience, its antecedents, and its outcomes. Moreover, additional papers were identified from reference lists from the retrieved papers. Authors made a conscious, joint, and iterative decision to consider each found paper as relevant, and to include them in this review.

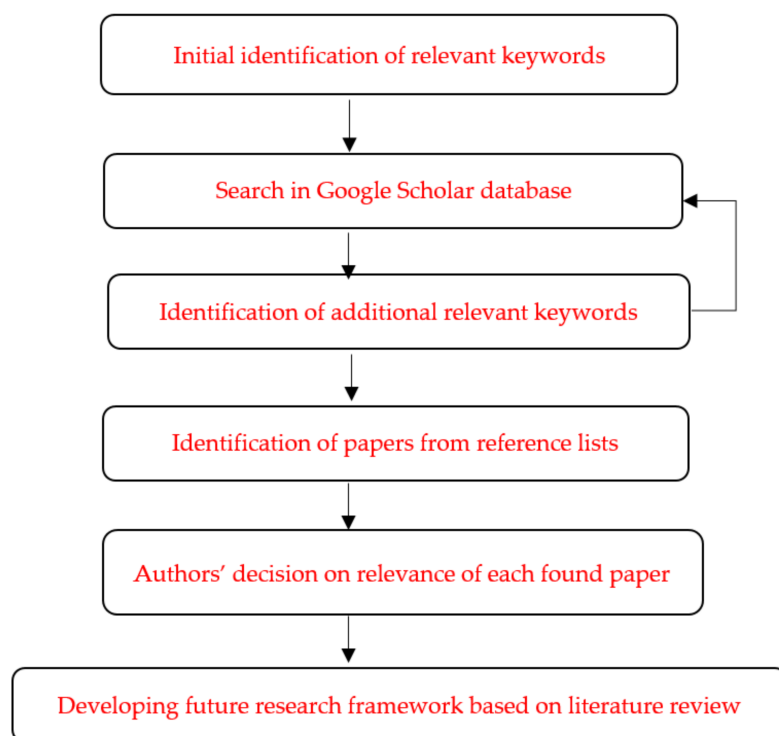


Figure 1. Flow chart of the literature search process.

### 3. Resilience Concept and Consumer Behavior

The phenomenon of resilience is, in academic research, understood in many ways and analyzed under different assumptions. In the social sciences, the concept of (engineering) resilience was introduced in the seminal work of [9], who defined resilience as the ability of a socio-ecological system to return to an equilibrium (steady-state) after a disturbance. Since then, resilience as a multidisciplinary concept has evolved through a wide variety of research across diverse academic disciplines. Several conceptual and review papers clarify the concept of resilience in various fields. For example, Klein, Nicholls and Thomalla [10] reviewed resilience to natural hazards, Brand and Jax [11] reviewed ecological resilience in sustainability science, and Nguyen et al. [12] evaluated community resilience. Our paper builds upon these studies, but within the specific context of consumer resilience to online privacy violation.

Holling's [9] notion of resilience implies resistance and sturdiness on one side, and adaptive capacity on the other. The behavior outcomes after the stressful event are generally understood as adaptations and may be positive, negative, or neutral [13]. Adaptive capacity is vital for the resilience of individuals who adjust based on immediate situation, knowing past conditions, or predicting future ones. Adaptive systems for human resilience include personal intelligence and motivation, macro-environment (e.g., regulatory systems), and knowledge, memories, and social interactions trusted sources of information [14]. The new balance (equilibrium) may be achieved either by 'bouncing back' [15] or 'bouncing forward' to a more desirable state (e.g., [16,17]). In line with this understanding of resilience, some authors [18] make distinctions between components of resilience, i.e., readiness and preparedness to a stressful event, response and adaptation to adverse conditions, and recovery or adjustment to the new after stress.

Nowadays, resilience is a 'boundary object' across fields, open to interpretation [11], meaning that most of the resilience literature develops resilience theories uniquely within their relevant research fields. However, empirical research to test the theoretical approaches is still rare.

In the theoretical research, one can distinguish studies of system resilience from individual resilience. Regarding the former, following a disturbance or stressful event,

functions are restored in a resilient system, although this new equilibrium may be different than before the disturbance. Building from this concept and keeping in mind the high complexity of individual behavior, consumer resilience might be regarded as system resilience, i.e., the consumer may be able to withstand, recover from, and reorganize after the disturbance [13].

On the other hand, individual resilience refers to processes patterns of positive adaptation during or following exposure to stressful events that may disrupt the normal functioning or development of a person [19]. The common attribute is a stressful event such as a natural disaster, pandemic, terrorist attack, human error, or equipment failure, which initiates rationalizing the resilience. However, even a small uncertainty or aberration from what is perceived as normal might be seen from an individual's point of view as a stressful event and a severe threat to the continuity of personal activity.

Early resilience studies gave more attention to the individual developmental processes whereby the individual's environment factors, which typically included their family, school, institution, or community, were connected for their influence on an individual, typically a child [20]. Personal qualities associated with individual resilience were identified as protectors from the negative influence of external stressors. In contrast, Rutter [21] interpreted individuals' resilience in terms of individual personality traits that were correlated with successful coping under stress, including reducing the risk of exposure and preventing the negative impact of risk factors. He further noted that, in a situation with the same disturbance dose and pattern, responses are highly heterogeneous [22]. In this research, we connected online privacy violation and resilience, and resilience is explored at the cross section of engineering, psychological, and individual contexts (see for example [23]). Thus, this research borrows resilience concepts from disaster management and organizational fields, which account for previous experience and any periods of regressive behavior. However, the foundational premises of resilience in consumer behavior come from scientific fields that explore the human behavior of individuals. From the individual viewpoint, resilience is understood as an interactive concept dealing with the aggregation of individuals' severe risk experiences with a different relatively favorable psychological outcomes despite stressors [24].

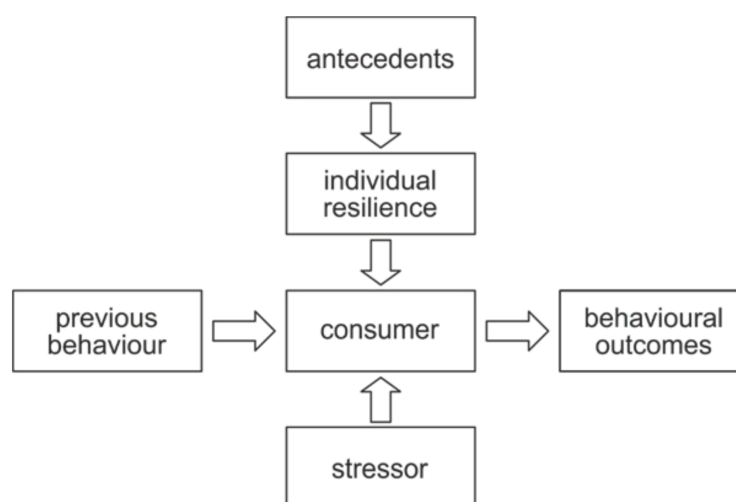
While the consumer behavior literature is exuberant, Solomon et al. [25] provided good historical review on this), and recent studies have shifted attention to their behavior in an online environment (e.g., e-consumer integrated behavior model developed by [26]; or extended model of online privacy concern by [27]). Furthermore, with increased popularity of virtual marketplaces, consumer behavioral studies in an online environment such as online shopping (e.g., [28]), e-commerce (e.g., [29]), and m-commerce (e.g., [30]), have gained importance due to the increasing development of online marketplaces. Recently, Islam [31] showed that consumer buying decisions in an online environment were affected by numerous factors, such as demographics, cultural, socioeconomic, consumer trust, their motivation, and perceived risk. What is more concerning, however, is that even though these behavior consequences grow in complexity in digitized environment, they remain relatively underexplored [32]. In 1999, more than 95% of digital consumers chose not to provide their sensitive personal information when online. This was predominantly the result of their privacy online concerns, which were affected by consumer digital literacy competences [33]. This increasing need for protecting digital consumers led to different propositions and policies for improvement of consumer digital literacy and for explicitly defining and simplifying statements on how to manage sensitive consumer data [34]. Anić et al. [27] showed that the purpose of data collection affects peoples' online privacy concerns and their behavior. As a response, national and municipal policymakers are continuously replacing traditional data collecting methods with various online services in many spheres, ranging from general data collection about their citizens to various e-services such as issuing birth certificates. Furthermore, this ongoing e-service development and implementation, primarily related to the public sector (often regarded as the smart city con-

cept [35,36]), must address consumer protection issues and require constant improvements in consumer digital literacy and any privacy awareness issues [30,37].

To conclude, consumer behavior is governed by several groups of factors, including psychological factors, socio-demographic characteristics, and external factors stemming from a consumer's micro- and macro-environment.

#### 4. Consumer Resilience to Online Privacy Violation: Conceptual Model

This section provides a thorough description, interpretation, and conclusion with regard to the experimental results related to every factor used in the model. The initial version of the conceptual model of the consumer resilience to online privacy violation assumes that consumer online behavior before and after a stressful event is defined by individual resilience, which is in turn affected by a set of antecedents (Figure 2).



**Figure 2.** The initial research concept.

A consumer's online activity in various dimensions is supposedly affected by the online privacy violation event. The research question of this paper is how does a consumer's online activity change after an online privacy breach (stressor), and what are the subsequent outcomes of online consumer activity in the particular dimensions (such as time spent on the Internet, types of transactions performed online, purpose of using the Internet, etc.). Note that the stressful event of a privacy breach affects individual consumers directly, and consumers' subjective perceptions of the online privacy breach would be sufficient to determining that a privacy violation occurred.

Privacy violation events could be *a posteriori* sorted into groups of less and more severe breaches, independent of the subjective classification that may be made by the victim. This could mitigate the risk of wrongly estimated concerns and perceptions. However, it is the estimated concern and perception that results in real behavioral outcomes. Namely, one type of privacy violation that is not perceived by individual A as a negative event might, on the other hand, be experienced by individual B as a serious attack on online privacy. Therefore, exposure to a privacy violation in the model should be a self-assessed subjective measure.

The individual consumer, when affected by the stressor, is at the same time resilient to a certain extent (hypothetically from zero resilience to full resilience). An individual's resilience is formed under the influence of various antecedents. Therefore, the proposed model should include antecedents of online consumer resilience, identify stressful events experienced as a privacy violation, and measure resilience by adaptation responses in terms of concrete online actions undertaken by a consumer.

Previous studies on individual resilience pointed at several contributing factors, or antecedents, that enhance resilience [38,39]. Among the variables that have been recognized

as important for resilience in different contexts, personality variables are one of the most important. Among the most important antecedents to personal resilience include different psychological factors (e.g., self-esteem, personality traits, locus of control, optimism, self-efficacy) (e.g., [38,40]), while other factors are of a socio-demographic type, and typically include income, education, age, occupation, and age (e.g., [41,42]). In addition, various resilience aspects should also be connected to different psychological well-being factors, as individuals with higher levels of resilience are in turn more successful at improving their psychological well-being [43]. Finally, recent evidence shows that various personality traits have a sizeable impact on resilience. For example, evidence shows that honesty, emotionality, humility, and openness to experiences influenced other personality factors, which then influenced resilience development, while extraversion, conscientiousness, and agreeableness are shown to affect innate and acquired resilience. However, individual resilience is seldomly affected only by personality traits (which are by nature quite rigid) but is also under the influence of wider micro- and macro-environmental factors. Examples of micro-environmental factors include social support, family relationships, peers, and stability; while macro-environmental factors generally include community, institutions, and cultural factors (e.g., [44]).

Translated into the model of researching the connection between consumer resilience and privacy violation online, these antecedents are systemized into five groups of variables: psychological factors, individual attitudes towards Internet usage, individual socio-demographic characteristics and digital literacy, micro-environmental factors, and macro-environmental factors.

#### *4.1. Antecedents of Consumer Resilience to Online Privacy Violation*

##### *4.1.1. Individual Psychological Factors*

Individual values shape the behavior and ideas representing personal life-guiding principles, which are worth considering as antecedents of consumer resilience. In the resilience research literature, numerous protective factors have been identified including hardiness [45], positive emotions [46], extraversion [47], spirituality [48], self-esteem [49], and positive affect [50]. In investigating psychological factors as antecedents in our model of consumer resilience to privacy violation in an online environment, self-efficacy emerges as a potentially significant variable [51] that assesses optimistic self-beliefs that help in coping with a variety of stressors in life. Schwarzer and Jerusalem [52] determined that if a person is dealing efficiently with unexpected events and solving problems, these abilities might be crucial to confronting a privacy violation event. Additionally, individuals' locus of control represents the degree to which they believe they have control over the event outcomes in their lives [53]. External control orientation regards to a belief that the event outcomes of personal actions stem from external circumstances—faith or luck—while internal control orientation refers to the belief that the outcomes of an individual's actions are driven by personal efforts and decisions. Self-esteem is also included in the model because people with higher self-esteem would not blame themselves for being a victim of an online privacy violation and would feel more capable of dealing with the adversity. Some studies claim that individual resilience is rarely attributable to personality traits, yet these factors are widely used in the resilience research. Personality traits are psychological factors describing an individual's characteristics that can influence psychological resilience [40,47]. The "Big Five" concept (e.g., [54]) separates individuals' personality into five traits: extraversion (social adaptability), openness (to experiences), agreeableness, conscientiousness, and neuroticism (emotional instability). Certain combinations of these traits can boost individual resilience before they even come across a stressful event. Past findings reported that (psychological) resilience was negatively associated with neuroticism, and positively related to extraversion and conscientiousness [47]. Another personality trait is optimism, i.e., maintaining positive expectations for future events or outcomes [42]. When encountering adversity, maintaining optimism for the future and hope [55] can provide the stamina to endure and to accept difficulties. Acknowledging the



need to adjust is attributed to an individual cognitive flexibility. Due to this characteristic a person sees alternatives, exhibits a willingness to adapt to new situations, and maintains self-efficacy in being flexible [56]. Active coping skills [57] are often employed by resilient individuals, including: (i) the cognitive component actively minimizing the appraisal of threats; and (ii) the behavioral component including positive statements, facing fears instead of avoiding them, and promoting efforts to ask for others' support.

#### 4.1.2. Individual Attitudes towards Internet Usage

It is important to differentiate individual traits from individual attitudes. There is evidence in the literature that attitudes shape behavior [58], so attitudes towards usage should be considered in the set of antecedents.

Privacy awareness is defined as individuals' consciousness regarding the importance of privacy online and threats in digital environment. Privacy awareness in an online environment includes awareness of privacy policy practices in both public and private sectors [59,60]. This relates to the individuals' desire for (sensitive) information control and to be familiarized about online privacy issues, given that everything posted online stays there forever and can potentially be (mis)used by a third party. The relationship between online privacy awareness and resilience to online privacy violation is speculated to work in the same direction. Higher awareness of online privacy policies and protocols might make Internet users more resilient.

Another factor important to consumer behavior online are the perceived benefits of Internet usage. This is a measure that assesses how beneficial it is for someone to use the Internet, i.e., to be a part of an online community [59,61]. Someone with a high personal interest to access online information or services might be willing to trade off, i.e., to tolerate potential online privacy violations, thus making the individual more resilient to any online privacy breaches in this sense. These individuals are constantly evaluating the risks and costs of providing their user data online against the benefits of participating in online interactions [62].

Resilience to online privacy breaches also relates to the degree of online privacy someone expects or demands. Previous studies have shown a direct correlation between this need and concerns for online privacy levels [60,63], which leads us to speculate that someone with a higher need for privacy in an online environment might be less resilient to any privacy breaches.

Computer anxiety is defined as a general technology fear and an aversion towards computerization, as well as concern and frustration about the perverse aspects of digitization [64], and it has been shown to negatively affect users' performance [65]. We speculate that an individual who is already very anxious and frustrated about an increased rate of digitalization would have a relatively low resilience towards online privacy breaches.

Privacy concern in an online environment represents apprehension and uneasiness of an individual regarding the (mis)use of their sensitive personal data [66], reflecting the degree of individuals' discomfort when online. We speculate that individuals with higher levels of concern regarding their privacy online might show lower resilience to privacy breaches online.

Control of personal information in and online environment and unauthorized secondary use of information reflects individuals' opinions on how their sensitive information should be managed online. It takes into consideration an individual's attitudes for various degrees of control over collection, sharing, and (mis)usage of their private information. Thus, it is regarded as an antecedent to individual resilience to privacy violation. Previous studies investigated the impact of perceived control of an individual [67] and their perceived ability to manage information [61]. Thus, we hypothesize that individuals who desire more control over their online information feel more "violated" in case of an online privacy breach, making this individual less resilient.

Online sharing of private information represents an individual's preferences about sharing his/her private sensitive information online. Past research indicated an indirect

association between willingness to provide private information online and privacy concerns [68]. We therefore theorized that individuals who are more willing to publicly share their information online would be more resilient to online privacy breaches.

Protective behavior refers to individual actions taken while in an online environment with the goal of protecting ones' identity and sensitive information, especially if a person perceives potential threats associated with online activity. According to [66], these protective behavior measures might include fabrication of personal online information (e.g., disguising individual identity by deliberately providing inaccurate or incomplete information); adopting various methods to safeguard online personal information (e.g., using various encryption algorithms and anti-tracking software); and purposefully withholding interaction with online content of form (e.g., refusing to fill-in forms on particular websites). Milne, Rohm, and Bahl [69] give a few examples of actions individuals might take to protect against online identity theft such as filling out forms from isolated accounts, rejection of website cookies, carefully reading through websites' privacy policies, and adding extra encryption to their e-mails. Hence, behavioral intention factors regarding data fabrication, protection, and withholding should be added to the proposed model. We speculate that the individual who utilizes more protective behavior techniques is more resilient to online privacy violations. In addition, the protective behavior processes and actions are more likely to be implemented by individuals facing higher-than-average risk levels [70].

#### 4.1.3. Individual Socio-Demographic Factors and Digital Literacy

Consumers' demographic characteristics can also explain resilience levels to privacy breaches in an online environment. Typically, gender, age, education, settlement type, occupation, and household size are included as explanatory variables in the consumer behavior model. As such, OECD [71] identified what it calls the "digital gender divide." Related research shows men to be more interested in digital technology, to be more digitally literate, more likely to take active control, and are more willing to take risks [72,73]. Furthermore, some studies indicated an increased likelihood for women to be exposed to various forms of abuse in an online environment [74], even though other studies claim that digital harassment is more common in men than women [75]. Given this research, we speculated that women are likely less resilient to online privacy breaches. In terms of age, we speculated that older Internet users tend to be less resilient to online privacy breaches than younger ones. These young "digital natives" have in general brighter outlooks on life and, more importantly, are more familiarized with different data collection practices and financial benefits of an online marketplace. On the other hand, older Internet users show a greater degree of sensitivity and desire to control every aspect of their online information [76]. If we look at income as an antecedent of resilience to online privacy breaches, we speculate that high earners are more resilient compared to those who earn less. Past research demonstrated that high earners in general show less concern about their online privacy compared to low earners [73,76]. Taking a closer look at the obtained education level, past research finds higher levels of online privacy concern for individuals with less education [77]. Finally, regarding the settlement type [78], data for 2019 indicate that about 48% of adults living in rural areas in European countries have basic or above basic digital skills. Moreover, Roberts et al. [79] stressed that rural areas significantly differed in the delivery and use of digital technologies, which is visible in the accessibility of different technologies, IT infrastructure, or IT education, which then affects their resilience in the digital world. We thus speculate that urban residents might show higher levels of resilience to online privacy breaches.

Moving on to the effects of digital skills (digital literacy) on resilience to online privacy breaches, Vandoninck, d'Haenens and Roe [80] investigated the factors that influence online resilience among young people in Europe. Their research showed that increased digital literacy levels correlated with greater resilience levels, including better coping strategies. They also emphasized the importance of the role of teachers and peers in increasing the level of online resilience among a younger population. Using a sample of students, similar



results were also obtained by [81], who proved a positive relationship between digital resilience and digital literacy. Moreover, Škrinjarić [82] showed that an improvement in digital skills correlated with a decline in online privacy concerns. Taking all this into consideration, we expect digital skills (digital literacy) to be positively associated to the individual resilience. Individuals with greater development of IT competences generally perform wider ranges of online activities and spend more time online but in a more secure manner, which might increase their resilience when dealing with potential online threats.

Like digital skills, a few studies suggested that an increased range of Internet user's activities may be inversely associated with online privacy concerns (e.g., [82]). Higher levels of familiarization with various online activities should lead to a reduction in computer anxiety and widen the usage of online services. Higher levels of engagement in a variety of online activities and improvements in digital competences should lead to an increased understanding of both the advantages and potential threats in an online environment [83]. However, even though increased diversity of online use and digital fluency is generally associated with reduction to online privacy threats, it may also increase individuals' exposure to more hidden threats, and hence the resilience may not increase for experienced users. The impact of consumers' time spent online is speculated to be positively associated with their resilience to online privacy violations.

#### 4.1.4. Micro-Environmental Factors

Micro-environmental factors comprise various elements of social support available to individuals and are considered one of the most important antecedents of resilience in different circumstances. In this context, social support is understood as the access to or availability of the assistance of others in time of adversity [84]. These factors include family, friends, peers, various organizations, etc. The key aspect of micro-environmental factors, and the main mechanism by which they affect resilience of an individual, is individuals' ability of interaction using their social support network in times of adversity [70]. In the specific context of resilience to online privacy breaches, these generalized concepts could be contextualized as access to a family member, friend, or peer with high computer literacy, and/or membership in an organization where some members exhibit high computer literacy.

#### 4.1.5. Macro-Environmental Factors

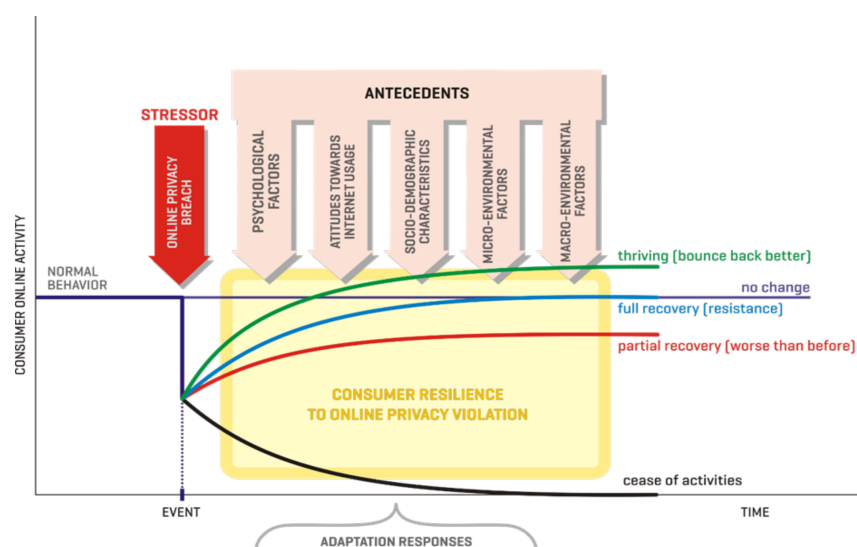
In general, macro-environmental factors refer to various laws, customs, and cultural practices that affect individuals' overall capacity to positively resolve real or perceived issues in time of adversity [70]. This group of factors exists at the community or society level and they are generated by social, political, institutional, and economic forces [85]. We posit that the social trust, both in institutions and in other people, affect individual behavior [86]. Further, consumers exhibiting less online privacy concern perceive that firms selling their products and services online are doing so in a responsible manner, and that legal regulations are at sufficient enough levels to ensure their privacy [87]. Perceptions of the effectiveness of government regulation of online activities, and the opinion that government regulations should be put in place to ensure and promote consumer online privacy [66], could affect consumer resilience to privacy breaches. In exploring consumer behavior online, the level of internet usage and digitalization present in the living and working environment of an individual is assumed to affect his/her resilience to privacy violation online as well. It is reasonable to suppose that a fact of living in a community with well-developed IT infrastructure, surrounded by other internet users, might nurture an individual's resilience to privacy violation online.

### 4.2. Outcomes of Consumer Resilience to Online Privacy Violation

Several outcomes are envisaged depending on an individual consumer's resilience, whereas the consumer's resilience is supposedly formed by antecedents and other determinants. Based on the conceptual model developed by [88], and the resilience framework

of [89], five types of reactions to privacy violations would be investigated in the model (Figure 3):

- No change in behavior, indicating full resilience to privacy breaches
- Full recovery, meaning that an individual bounces back to his/her normal activity as it was before the stressful event happened
- Partial recovery to the worse-than-before level
- Recovery at the bounce-back-better level (the hypothetical case that after a negative event has passed without severe consequences the consumer stops worrying about privacy violation and intensifies online activities)
- A complete cessation of previous activities online related to the privacy violation event. This last reaction is the worst-case scenario of adaptation response to privacy breach and denotes no resilience at all



**Figure 3.** Conceptual model of consumer resilience to privacy violation online.

Variations in resilience would be measured by observing how consumer behavior recovers after taking adaptation actions during a reasonable amount of time.

When considering behavioral outcomes, it is imperative to consider possible inconsistencies between behavior and attitudes. Although behavior might be recovered after a privacy breach incident, attitudes might remain unrecovered and an inconsistency between behavior and attitudes might be observed. This phenomenon is known in the literature as inconsistency between attitude components [90,91]. Therefore, it might be useful to measure not only behavior but attitudes as well, as one of the possible elements of an outcome.

Resilience is psychology and social systems, regarded as capacity to adjust and flourish, is frequently conceived as a competence that a group or individual use when facing disturbance (stressor) that allows reaching a functionality level designated to be classified as “good” [92]. Hence, this argument corresponds to the “full recovery” outcome in our model. Antecedents are assumed to directly affect resilience; resilience is a latent variable measured using different scales, which then affects outcomes. However, some antecedents can directly affect outcomes, regardless of resilience (e.g., if one must use the Internet very frequently at work, a change in behavior is unlikely to be observed, though a change in attitudes may be).

## 5. Summary and Future Directions

In order to assess consumer behavior after experiencing an online privacy violation, we borrowed and adapted from the resilience and consumer behavior literature the idea that after a stressful event, individual consumer behavior is restored, but not necessarily in the same way as before the event. We argued here that a set of individual characteristics and

micro- and macro-environmental conditions affect the specific consumer behavior outcomes and propose a research model worth empirically testing to examine functionalities and the concept developed in this work. It remains to be seen which variables strengthen the adaptive or coping capacity of an individual or affect the perceived risk of an online privacy violation.

The proposed conceptual model of individual consumer resilience to privacy violation in an online environment offers multiple opportunities for future research. In the context of qualitative research methodology, focus groups, and in-depth interviews could be applied since these methods have the potential to provide useful and more detailed insights into the relationship between model variables. Moreover, these research methods can be used to evaluate actual consumer behavior after a privacy breach has occurred. The proposed research model could also be empirically tested by a quantitative research methodology approach. Using a method such as a survey could lead to a more thorough understanding of the model as well as the relationship between the model variables. The research model can also be tested using an experimental research method primarily conducted in a laboratory setting. In addition, a longitudinal research approach should also be taken into consideration since it would allow for monitoring of the model as well as possible changes in the relationship between variables over time. Finally, since the research model of consumer resilience to online privacy violation has been proposed as a general one, future research studies could focus on examining the model applicability to specific industries and/or socio-cultural and economic contexts.

**Author Contributions:** Conceptualization, J.B., E.R., and B.Š.; methodology, J.B., E.R., S.S., and B.Š.; writing—original draft preparation, J.B. and B.Š.; writing—review and editing J.B., E.R., S.S., and B.Š.; funding acquisition, J.B. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work has been fully supported by the Croatian Science Foundation under Project IP-2019-04-7886.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** No new data were created or analyzed in this study. Data sharing is not applicable to this article.

**Acknowledgments:** The authors appreciate the useful comments of Zvezdan Penezić and Šime Lugović, as well as the assistance of Allison M. Carragher.

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

## References

1. Bhattacharyya, A.; Belk, R.W. Consumer resilience and subservience in technology consumption by the poor. *Consum. Mark. Cult.* **2019**, *22*, 489–507. [\[CrossRef\]](#)
2. Kaaniche, N.; Laurent, M.; Belguith, S. Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *J. Netw. Comput. Appl.* **2020**, *171*, 102807. [\[CrossRef\]](#)
3. Çatak, F.Ö.; Mustacoglu, A.F. CPP-ELM: Cryptographically privacy-preserving extreme learning machine for cloud systems. *Int. J. Comput. Intell. Syst.* **2018**, *11*, 33–44. [\[CrossRef\]](#)
4. Heurix, J.; Zimmermann, P.; Neubauer, T.; Fenz, S. A taxonomy for privacy enhancing technologies. *Comput. Secur.* **2015**, *53*, 1–17. [\[CrossRef\]](#)
5. Ferrari, R. Writing narrative style literature reviews. *Med. Writ.* **2015**, *24*, 230–235. [\[CrossRef\]](#)
6. Huelin, R.; Iheanacho, I.; Payne, K.; Sandman, K. What's in a name? Systematic and nonsystematic literature reviews, and why the distinction matters. *Evidence* **2015**, 34–37.
7. McDougall, R. Reviewing Literature in Bioethics Research: Increasing Rigour in Non-Systematic Reviews. *Bioethics* **2015**, *29*, 523–528. [\[CrossRef\]](#)
8. Snyder, H. Literature review as a research methodology: An overview and guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [\[CrossRef\]](#)
9. Holling, C.S. Resilience and stability of ecological systems. *Annu. Rev. Ecol. Syst.* **1973**, *4*, 1–23. [\[CrossRef\]](#)
10. Klein, R.J.T.; Nicholls, R.J.; Thomalla, F. Resilience to natural hazards: How useful is this concept? *Glob. Environ. Chang. Part B: Environ. Hazards* **2003**, *5*, 35–45. [\[CrossRef\]](#)

11. Brand, F.S.; Jax, K. Focusing the meaning(s) of resilience: Resilience as a descriptive concept and a boundary object. *Ecol. Soc.* **2007**, *12*, 23. [\[CrossRef\]](#)
12. Nguyen, H.L.; Akerkar, R. Modelling, Measuring, and Visualising Community Resilience: A Systematic Review. *Sustainability* **2020**, *12*, 7896. [\[CrossRef\]](#)
13. Martin-Breen, P.; Anderies, J.M. *Resilience: A Literature Review*; Institute of Development Studies (IDS): Brighton, UK, 2011.
14. Norris, F.; Stevens, S.; Pfefferbaum, B.; Wyche, K.; Pfefferbaum, R. Community Resilience as a Metaphor, Theory, Set of Capacities and Strategy for Disaster Readiness. *Am. J. Community Psychol.* **2008**, *41*, 127–150. [\[CrossRef\]](#) [\[PubMed\]](#)
15. Wildavsky, A. *Searching for Safety*; Transaction Publishers: New Brunswick, NJ, USA, 1988.
16. Davoudi, S.; Shaw, K.; Haider, L.J.; Quinlan, A.E.; Peterson, G.D.; Wilkinson, C.; Fünfgeld, H.; McEvoy, D.; Porter, L.; Davoudi, S. Resilience: A Bridging Concept or a Dead End? “Reframing” Resilience: Challenges for Planning Theory and Practice Interacting Traps: Resilience Assessment of a Pasture Management System in Northern Afghanistan Urban Resilience: What Does it Mean in Planning Practice? Resilience as a Useful Concept for Climate Change Adaptation? The Politics of Resilience for Planning: A Cautionary Note. *Plan. Theory Pract.* **2012**, *13*, 299–333.
17. Manyena, S.B. The concept of resilience revisited. *Disasters* **2006**, *30*, 434–450. [\[CrossRef\]](#)
18. Ponomarov, S.Y.; Holcomb, M.C. Understanding the concept of supply chain resilience. *Int. J. Logist. Manag.* **2009**, *20*, 124–143. [\[CrossRef\]](#)
19. Masten, A.S.; Obradovic, J. Disaster preparation and recovery: Lessons from research on resilience in human development. *Ecol. Soc.* **2007**, *13*, 9. [\[CrossRef\]](#)
20. Ungar, M. Social Ecologies and their Contribution to Resilience. In *The Social Ecology of Resilience*; Ungar, M., Ed.; Springer: New York, NY, USA, 2012; pp. 13–32.
21. Rutter, M. Psychosocial resilience and protective mechanisms. *Am. J. Orthopsychiatry* **1987**, *57*, 316–331. [\[CrossRef\]](#)
22. Rutter, M. Resilience: Causal Pathways and Social Ecology. In *The Social Ecology of Resilience*; Ungar, M., Ed.; Springer: New York, NY, USA, 2012; pp. 33–42.
23. Bhamra, R.; Dani, S.; Burnard, K. Resilience: The concept, a literature review and future directions. *Int. J. Prod. Res.* **2011**, *49*, 5375–5393. [\[CrossRef\]](#)
24. Rutter, M. Implications of resilience concepts for scientific understanding. *Ann. NY Acad. Sci.* **2006**, *1094*, 1–12. [\[CrossRef\]](#)
25. Solomon, M.R.; Bamossy, G.J.; Askegaard, S.T.; Hogg, M.K. *Consumer Behavior. A European Perspective*, 5th ed.; Pearson: Harlow, UK, 2013.
26. Dennis, C.; Merrilees, B.; Jayawardhena, C.; Wright, L.T. E-consumer behavior. *Eur. J. Mark.* **2009**, *43*, 1121–1139. [\[CrossRef\]](#)
27. Anić, I.D.; Budak, J.; Rajh, E.; Recher, V.; Škare, V.; Škrinjaric, B. Extended model of online privacy concern: What drives consumers’ decisions? *Online Inf. Rev.* **2018**, *43*, 799–817. [\[CrossRef\]](#)
28. Demangeot, C.; Broderick, A.J. Conceptualising consumer behavior in online shopping environments. *Int. J. Retail Distrib. Manag.* **2007**, *35*, 878–894. [\[CrossRef\]](#)
29. Oliveira, M.G.; Toaldo, A.M.M. New times, new strategies: Proposal for an additional dimension to the 4 P’s for e-commerce dot-com.com. *J. Inf. Syst. Technol. Manag.* **2015**, *12*, 107–124. [\[CrossRef\]](#)
30. Sharif, M.S.; Shao, B.; Xiao, F.; Saif, M.K. The impact of psychological factors on consumers trust in adoption of m-commerce. *Int. Bus. Res.* **2014**, *7*, 148–155. [\[CrossRef\]](#)
31. Islam, S. Factors Influencing Customer’s Intention to Adopt Online Shopping: A Holistic Approach. *Int. J. Bus. Technopreneurship* **2019**, *9*, 57–66.
32. Ginosar, A.; Ariel, Y. An analytical framework for online privacy research: What is missing? *Inf. Manag.* **2017**, *54*, 948–957. [\[CrossRef\]](#)
33. Hoffman, D.; Novak, T.A.; Peralta, M. Building Consumer Trust Online. *Commun. ACM* **1999**, *42*, 80–85. [\[CrossRef\]](#)
34. Mosco, V. Citizenship in a Post-Internet World. In *Becoming Digital*; Mosco, V., Ed.; Emerald Publishing Limited: Bentley, UK, 2017; pp. 175–212.
35. Van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480. [\[CrossRef\]](#)
36. Myeong, S.; Jung, Y.; Lee, E. A Study on Determinant Factors in Smart City Development: An Analytic Hierarchy Process Analysis. *Sustainability* **2018**, *10*, 2606. [\[CrossRef\]](#)
37. Gazzola, P.; Colombo, G.; Pezzetti, R.; Nicolescu, L. Consumer Empowerment in the Digital Economy: Availing Sustainable Purchasing Decisions. *Sustainability* **2017**, *9*, 693. [\[CrossRef\]](#)
38. Joseph, S.; Linley, P.A. Growth following adversity: Theoretical perspectives and implications for clinical practice. *Clin. Psychol. Rev.* **2006**, *26*, 1041–1053. [\[CrossRef\]](#) [\[PubMed\]](#)
39. Herrman, H.; Stewart, D.E.; Diaz-Granados, N.; Berger, E.L.; Jackson, B.; Yuen, T. What is resilience? *Can. J. Psychiatry* **2011**, *56*, 258–265. [\[CrossRef\]](#) [\[PubMed\]](#)
40. Nakaya, M.; Oshio, A.; Kaneko, H. Correlations for Adolescent Resilience Scale with Big Five Personality Traits. *Psychol. Rep.* **2006**, *98*, 927–930. [\[CrossRef\]](#) [\[PubMed\]](#)
41. Campbell-Sills, L.; Forde, D.R.; Stein, M.B. Demographic and childhood environmental predictors of resilience in a community sample. *J. Psychiatr. Res.* **2009**, *43*, 1007–1012. [\[CrossRef\]](#) [\[PubMed\]](#)
42. Carver, C.S.; Scheier, M.F.; Segerstrom, S.C. Optimism. *Clin. Psychol. Rev.* **2010**, *30*, 879–889. [\[CrossRef\]](#)
43. Fredrickson, B.L. The role of positive emotions in positive psychology: The broaden-and-build theory of positive emotions. *Am. Psychol.* **2001**, *56*, 218–226. [\[CrossRef\]](#)



44. Luthar, S.S.; Cicchetti, D. The construct of resilience: Implications for interventions and social policies. *Dev. Psychopathol.* **2000**, *12*, 857–885. [\[CrossRef\]](#)
45. Bonanno, G.A. Loss, trauma, and human resilience: Have we underestimated the human capacity to thrive after extremely aversive events? *Am. Psychol.* **2004**, *59*, 20–28. [\[CrossRef\]](#)
46. Tugade, M.M.; Fredrickson, B.L. Resilient individuals use positive emotions to bounce back from negative emotional experiences. *J. Personal. Soc. Psychol.* **2004**, *86*, 320–333. [\[CrossRef\]](#)
47. Campbell-Sills, L.; Cohan, S.L.; Stein, M.B. Relationship of resilience to personality, coping, and psychiatric symptoms in young adults. *Behav. Res. Ther.* **2006**, *44*, 585–599. [\[CrossRef\]](#) [\[PubMed\]](#)
48. Bogar, C.B.; Hulse-Killacky, D. Resiliency determinants and resiliency processes among female adult survivors of childhood sexual abuse. *J. Couns. Dev.* **2006**, *84*, 318–327. [\[CrossRef\]](#)
49. Kidd, S.; Shahar, G. Resilience in homeless youth: The key role of self-esteem. *Am. J. Orthopsychiatry* **2008**, *78*, 163–172. [\[CrossRef\]](#) [\[PubMed\]](#)
50. Zautra, A.J.; Johnson, L.M.; Davis, M.C. Positive affect as a source of resilience for women in chronic pain. *J. Consult. Clin. Psychol.* **2005**, *73*, 212–220. [\[CrossRef\]](#)
51. Gu, Q.; Day, C. Teachers' resilience: A necessary condition for effectiveness. *Teach. Teach. Educ.* **2007**, *23*, 1302–1316. [\[CrossRef\]](#)
52. Schwarzer, R.; Jerusalem, M. Generalised Self-Efficacy Scale. In *Measures in Health Psychology: A User's Portfolio. Causal Control and Beliefs*; Weinman, W., Johnston, M., Eds.; Nfer-Nelson: Windsor, UK, 1995; pp. 35–37.
53. Rotter, J.B. Generalized expectancies for internal vs. external control of reinforcement. *Psychological Monogr.* **1966**, *80*, 1–28. [\[CrossRef\]](#)
54. Goldberg, L.R. The development of markers for the Big-Five factor structure. *Psychol. Assessment* **1992**, *7*, 26–42. [\[CrossRef\]](#)
55. Snyder, C. The past and possible futures of hope. *J. Soc. Clin. Psychol.* **2000**, *19*, 11–29. [\[CrossRef\]](#)
56. Martin, M.M.; Rubin, R.B. A new measure of cognitive flexibility. *Psychol. Rep.* **1995**, *76*, 623–626. [\[CrossRef\]](#)
57. Bolger, N. Coping as a personality process: A prospective study. *J. Personal. Soc. Psychol.* **1990**, *59*, 525–537. [\[CrossRef\]](#)
58. Glasman, L.R.; Albarracín, D. Forming attitudes that predict future behavior: A meta-analysis of the attitude-behavior relation. *Psychol. Bull.* **2006**, *132*, 778–822. [\[CrossRef\]](#) [\[PubMed\]](#)
59. Malhotra, N.; Kim, S.; Agarwal, J. Internet users' information privacy concerns (IUIPC): The construct, the scale and a causal model. *Inf. Syst. Res.* **2004**, *15*, 336–355. [\[CrossRef\]](#)
60. Xu, H.; Dinev, T.; Smith, H.J.; Hart, P. Examining the formation of individual's privacy concerns: Toward an integrative view. In *Proceedings of the 29th International Conference on Information Systems, Paris, France, 14–17 December 2008*; Association for Information Systems Electronic Library (AISeL): Paris, France, 2008; pp. 1–16.
61. Dinev, T.; Hart, P. Internet Privacy Concerns and Their Antecedents, Measurement Validity and a Regression Model. *Behav. Inf. Technol.* **2004**, *23*, 413–422. [\[CrossRef\]](#)
62. Teubner, T.; Flath, C.M. Privacy in the sharing economy. *J. Assoc. Inf. Syst.* **2019**, *20*, 213–242. [\[CrossRef\]](#)
63. Yao, M.Z.; Rice, R.E.; Wallis, K. Predicting User Concerns about Online Privacy. *J. Am. Soc. Inf. Sci. Technol.* **2007**, *58*, 710–722. [\[CrossRef\]](#)
64. Parasuraman, S.; Igarbaria, M. An examination of gender differences in the determinants of computer anxiety and attitudes toward microcomputers among managers. *Int. J. Man-Mach. Stud.* **1990**, *32*, 327–340. [\[CrossRef\]](#)
65. Thomas, J. Factors affecting computer anxiety and its effects on ease of use of business software. Managing Social and Economic Change with Information Technology. In *Proceedings of the 1994 Information Resources Management Association. International Conference, San Antonio, TX, USA, 22–25 May 1994*; Khosrowpour, M., Ed.; IDEA Group Publishing: London, UK, 1994; pp. 51–52.
66. Lwin, M.; Wirtz, J.; Williams, J.D. Consumer Online Privacy Concerns and Responses: A Power–Responsibility Equilibrium Perspective. *J. Acad. Mark. Sci.* **2007**, *35*, 572–585. [\[CrossRef\]](#)
67. Milne, G.R.; Boza, M.E. Trust and Concern in consumers' perceptions of marketing information management practices. *J. Interact. Mark.* **1999**, *13*, 5–24. [\[CrossRef\]](#)
68. Bandyopadhyay, S. Online privacy concerns of Indian consumers. *Int. Bus. Econ. Res. J.* **2011**, *10*, 93–100. [\[CrossRef\]](#)
69. Milne, G.R.; Rohm, A.J.; Bahl, S. Consumers' protection of online privacy and identity. *J. Consum. Aff.* **2004**, *38*, 217–232. [\[CrossRef\]](#)
70. Ungar, M. The Social Ecology of Resilience: Addressing Contextual and Cultural Ambiguity of a Nascent Construct. *Am. J. Orthopsychiatry* **2011**, *81*, 1–17. [\[CrossRef\]](#) [\[PubMed\]](#)
71. OECD. Bridging the Digital Gender Divide. 2018. Available online: <http://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf> (accessed on 25 October 2020).
72. Fogel, J.; Nehmad, E. Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns. *Comput. Hum. Behav.* **2009**, *25*, 153–160. [\[CrossRef\]](#)
73. Zhang, R.; Chen, J.Q.; Lee, C.J. Mobile commerce and consumer privacy concerns. *J. Comput. Inf. Syst.* **2013**, *53*, 31–38. [\[CrossRef\]](#)
74. Grubbs Hoy, M.; Milne, G. Gender differences in privacy-related measures for young adult Facebook users. *J. Interact. Advert.* **2010**, *10*, 28–45.
75. Nadim, M.; Fladmoe, A. Silencing Women? Gender and Online Harassment. *Soc. Sci. Comput. Rev.* **2019**. [\[CrossRef\]](#)
76. Zukowski, T.; Brown, I. Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns. In *2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries*; ACM: New York, NY, USA, 2007; pp. 197–204.
77. O'Neil, D. Analysis of Internet Users' Level of Online Privacy Concerns. *Soc. Sci. Comput. Rev.* **2001**, *19*, 17–31. [\[CrossRef\]](#)



78. European Commission. *Urban and Rural Living in the EU*; EC-European Commission: Brussels, Belgium, 2020.
79. Roberts, E.; Beel, D.; Philip, L.; Townsend, L. Rural resilience in a digital society: Editorial. *J. Rural Stud.* **2017**, *54*, 355–359. [[CrossRef](#)]
80. Vandoninck, S.; d’Haenens, L.; Roe, K. Online Risks—Coping strategies of less resilient children and teenagers across Europe. *J. Child. Media* **2013**, *7*, 60–78. [[CrossRef](#)]
81. Tran, T.; Ho, M.-T.; Pham, T.-H.; Nguyen, M.-H.; Nguyen, K.-L.P.; Vuong, T.-T.; Nguyen, T.-H.T.; Nguyen, T.-D.; Nguyen, T.-L.; Khuc, Q.; et al. How Digital Natives Learn and Thrive in the Digital Age: Evidence from an Emerging Economy. *Sustainability* **2020**, *12*, 3819. [[CrossRef](#)]
82. Škrinjaric, B. Internet literacy in an online environment: Influence of Internet skills on Internet privacy. In Proceedings of the fourth International Conference: The Challenges of today, Šibenik, Croatia, 10–12 October 2019; Filiposki, O., Metodijeski, D., Zlatovic, D., Eds.; Polytechnic of Šibenik: Šibenik, Croatia, 2019; pp. 165–178.
83. Rice, R.E. Influences, usage, and outcomes of Internet health information searching: Multivariate results from the Pew surveys. *Int. J. Med Inform.* **2006**, *75*, 8–28. [[CrossRef](#)]
84. Scoloveno, R. A Concept Analysis of the Phenomenon of Resilience. *J. Nurs. Care* **2016**, *5*, 1–5. [[CrossRef](#)]
85. Windle, G. What is resilience? A review and concept analysis. *Rev. Clin. Gerontol.* **2011**, *21*, 152–169. [[CrossRef](#)]
86. Naef, M.; Schupp, J. *Measuring Trust: Experiments and Surveys in Contrast and Combination*. IZA Discussion Paper Series, IZA Discussion paper No. 4087; Institute for the Study of Labor (IZA): Bonn, Germany, 2009.
87. Wirtz, J.; Lwin, M.; Williams, J.D. Causes and consequences of consumer online privacy concern. *Int. J. Serv. Ind. Manag.* **2007**, *18*, 326–348. [[CrossRef](#)]
88. Raab, C.D.; Jones, R.; Székely, I. Surveillance and resilience in theory and practice. *Media Commun.* **2015**, *3*, 21–41. [[CrossRef](#)]
89. Combaz, E. *Disaster Resilience: Topic Guide*; Governance and Social Development Resource Centre (GSDRC); University of Birmingham: Birmingham, UK, 2014.
90. Maio, G.R.; Esses, V.M.; Bell, D.W. Examining Conflict between Components of Attitudes: Ambivalence and Inconsistency are Distinct Constructs. *Can. J. Behav. Sci.* **2000**, *32*, 71–83. [[CrossRef](#)]
91. Rosenberg, M.J. A Structural Theory of Attitude Dynamics. *Public Opin. Q.* **1960**, *24*, 319–340. [[CrossRef](#)]
92. Longstaff, P.H.; Koslowskib, T.G.; Geoghegan, W. Translating resilience: A framework to enhance communication and Implementation. In Proceedings of the 5th Resilience Engineering Association Symposium on Resilience Engineering, Soesterberg, The Netherlands, 24–27 June 2013; pp. 1–8.