Journal of Cybersecurity and Privacy

MDPI

Article

Experiential Transformation in Privacy Behavior: A New Framework for Privacy Behavior Enhancement

Ioannis Paspatis * and Aggeliki Tsohou

Department of Informatics, Ionian University, 49100 Corfu, Greece; atsohou@ionio.gr
* Correspondence: ipaspatis@ionio.gr; Tel.: +30-26610-87760

Abstract: Multiple studies have demonstrated that the conventional method of learning is suboptimal when our goal is to enhance individuals' genuine privacy behavior. This study introduces a framework for transforming privacy behavior, with the objective of enhancing individuals' privacy practices to a higher level of confidentiality. We performed an experiment on a limited number of people to validate the efficacy of our suggested transformation framework. This framework combined determining aspects of privacy behavior with experiential behavior modification methodologies such as neutral stimuli (e.g., cognitive behavioral transformation—CBTx), practical assessments and motivational interviews from other disciplines. While these methods have proven effective in fields like psychology and sociology, they have not yet been applied to the realm of Information Computer and Technology (ICT). In this study, we have effectively demonstrated the efficacy of the proposed framework through a five-phase experiment. The suggested framework has the potential to be advantageous for educational institutions, including both public and private schools as well as universities, to construct new frameworks or develop new methodologies regarding individuals' privacy behavior transformation to a more protective one. Furthermore, our framework offers a conducive environment for further investigation into privacy behavior transformation methodologies.

Keywords: privacy behavior; privacy behavior transformation; privacy attitude; privacy behavior transformation framework

Citation: Paspatis, I.; Tsohou, A. Experiential Transformation in Privacy Behavior: A New Framework for Privacy Behavior Enhancement. *J. Cybersecur. Priv.* **2024**, *4*, 76–104. https://doi.org/10.3390/jcp4010005

Academic Editors: Thomas Hupperich, Martin Degeling, Luis Javier García Villalba, Maryline Laurent and Georgios Kambourakis

Received: 29 December 2023
Revised: 4 February 2024
Accepted: 5 February 2024
Published: 7 February 2024

1. Introduction

The recent advances in technology, such as internet-connected wearables, augmented reality, mobile devices, and the widespread presence of social media in our everyday lives, our singularity and individuality are constantly being put on display for the world to see [1]. Data can be obtained from individuals as well as businesses in a variety of different methods, and sometimes it happens even without our knowledge [2]. One way this can happen is via the gadgets that are connected to the Internet of Things (IoT) [3], and another is when we voluntarily expose ourselves on social networking sites such as posting a personal photo or other personal information. The provision of such advanced information services has triggered researchers to examine the phenomenon of privacy behavior. Privacy Behavior actions include personal information disclosure or the application of privacy-protective controls, or the configuration of privacy settings [4].

In the past ten years, there has been a discernible rise in the amount of studies conducted on understanding the factors that influence individuals' privacy behavior [5–9]. Researchers, software companies, companies that provide information security, and individuals are interested in findings ways to improve the privacy behavior of information and communication technology (ICT) users. Despite the fact that many ICT users claim to be concerned about their privacy, research from a number of different studies has revealed that the same individuals nonetheless reveal a significant amount of personal information online. The term "privacy paradox" was coined to describe this situation by a number of scholars [5–8]. Self-disclosure of information may have negative consequences on our lives,

such as becoming a victim of identity theft and impersonation. Moreover, third parties may exploit this information for their own benefit, such as targeted advertising practices [10,11] or even affecting people's voting opinion [12].

A number of studies have been conducted in an effort to determine the elements that contribute to the psychological, sociological, and behavioral motivations of ICT users' privacy-related actions [5,6]. Numerous scholars have identified a range of factors that may have an impact on privacy behavior [7,8,13]. Consequently, by influencing these factors, it may be possible to influence ICT users' privacy behavior, including their tendency to disclose personal information, employ privacy-protective measures, or adjust privacy settings [7,8]. Although there exist many scattered privacy behavior models, an integrated framework that may effectively facilitate such change is missing in the literature. In order to address this gap, in this paper, we integrate existing privacy behavior determinants and we rely on experiential behavior transformation theories, so as to develop a novel experiential privacy behavior transformation framework towards enabling ICT users' privacy-protective behavior. In summary, our paper addresses the following research questions:

Research Question 1: Can an individual's privacy behavior be transformed through experiential methods?

Research Question 2: Which experience method is more effective in transforming an individual's privacy behavior?

To address the above research questions, in this paper, we suggest and validate the effectiveness of a novel privacy behavior transformation framework. This framework and its validation consist of an experiment that includes a variety of methods such us conducting questionnaires, interviews and applying behavioral transformation methodologies (such as experiential methodologies), as described in the following sections. These theories and methods are based on concrete scientific theories and methods from other disciplines such as cognitive behavior transformation methods.

After the introduction, this paper continues with the literature review on privacy behavior theories and privacy behavior determinant factors. In Section 3, we investigate the theoretical background in experiential theories. In Section 4, we propose our experiential privacy behavior transformation framework, while we provide our methodology to empirically test the proposed framework in Section 5. In Section 6, we present the results of our empirically tests. Finally, Section 7 concludes this paper and provides implications and future research.

2. The Literature Review

2.1. Privacy Behavior Theories

Two primary theories have been used for understanding privacy behavior, including the privacy calculus theory and the privacy paradox. The privacy calculus theory suggests that individuals engage in a rational evaluation of costs and benefits when making decisions regarding their privacy [14]. Put simply, individuals assess the potential advantages of revealing their personal information in comparison to the potential drawbacks, such as the possibility of identity theft or discriminatory treatment. The privacy paradox theory refers to the discrepancy between people's stated privacy concerns and their actual privacy behavior [5]. For example, people may say that they care about their privacy, but they may still disclose a lot of personal information online.

Additionally, we encountered references to other theories, namely the "theory of privacy as a resource" and the "theory of privacy as a right". The perspective known as the "theory of privacy as a resource" posits that privacy is a valuable asset that may be leveraged to attain many objectives, including but not limited to social standing and financial benefits. As an illustration, individuals may have a propensity to divulge their personal information as a result of incentives, such as price reductions or complimentary merchandise. The perspective known as the "theory of privacy as a right" posits that privacy is an inherent and essential entitlement of individuals, which ought to be safeguarded against encroachments by both governmental and corporate entities. Many countries have

laws to guard this right by suggesting directives such as OECD Privacy Guidelines or implementing laws such as the General Data Protection Regulation (GDPR), which is the regulation on data protection and privacy in the European Union [15], the corresponding Brazilian law [16] called General Data Protection Law Lei Geral de Proteção de Dados (LGDP), the Personal Information Protection Act (PIPA) in Canada [17] and Personal Data Protection Act (PDPA) in Singapore [18].

Each of these theories possesses distinct advantages and limitations. The privacy calculus theory provides a valuable framework for comprehending the various determinants that shape individuals' privacy-related choices. However, it falls short in acknowledging the emotional and social dimensions of privacy. The concept of the privacy paradox serves as a valuable framework for comprehending the incongruity between individuals' privacy-related behaviors and their expressed worries. However, it falls short in elucidating the underlying reasons for this disparity. Theoretical frameworks that conceptualize privacy as a resource offer insight into individuals' motivations for divulging personal information. However, these frameworks fail to fully acknowledge the inherent value of privacy as an independent and significant entity. Theoretical frameworks concerning privacy as a fundamental right play a crucial role in safeguarding privacy against encroachments. However, these theories offer limited assistance in navigating the delicate equilibrium between privacy and other societal objectives, such as security or efficiency.

2.2. Privacy Behavior Determinant Factors

Previous studies have explored the determinants of privacy behavior, often employing pertinent theoretical frameworks, such as the protection motivation theory [19]. Other studies have investigated the variables that influence individuals' privacy behavior and developed relevant research models.

Many studies propose that gender significantly influences privacy behavior [20–24]. Their research indicated that gender significantly influences the extent to which individuals disclose personal information on the internet, with age being a contributing factor. As an illustration, women usually display a higher frequency of posting on their preferred social network and impose less limitations on privacy compared to men. The aforementioned studies are also incorporated into the research conducted by Paspatis et al. [13], who consolidated all of the factors determining privacy behavior into a single study. Other studies verify that age is also a contributing factor [8,20,21,25,26]. For example, it has been shown that as they grow older, adolescent males prefer to decrease the amount of information they share on online social networks (OSNs) and remove tags from their earlier photographs [27]. Further, relevant works have asserted that the perception of privacy risks [27–29] and their privacy concerns [30–37] also have a noteworthy impact on privacy-related behaviors. Another factor that appears to influence privacy behavior is the potential financial benefits or exchanges that individuals can obtain through the sharing of their personal data with providers. Previous research shows that individuals who state that they wish to protect their personal data are willing to disclose personal information in contrast to those statements in case of financial or other non-financial exchanges [25,30,33,38–41]. Financial and non-financial transactions (such as a monetary transaction involving personal data disclosure is the provision of a 10-euro advance or, additionally, the usage of a mobile application game that advertises to be free of advertisements but necessitates the reveal of personal data) have the potential to influence individuals to overcome their concerns and willingly disclose their personal information to third parties, as well as agree to the terms and conditions presented to them [31,38,41–45]. The literature has also demonstrated that privacy behavior is influenced by the necessary disclosure of information to complete tasks or fulfill practical needs. For example, users are requested to present identification documents to an aviation company when traveling [30,46] or to provide medical records, such as a COVID-19 vaccination certificate, for medical purposes [47]. The same may happen for psychological needs, such as psychological charging [35,46,48], for example when downloading a mobile application for entertainment purposes [49].

Furthermore, socialization needs (e.g., social media) may also drive personal information disclosure [34,35]. Other studies have examined the impact of education [45,50], the allocation of time for making privacy behavior choices [51,52], and the use of visualization techniques [36,51,53] on privacy behavior.

Further to these works, previous research has attempted to aggregate the identified factors that affect privacy behavior in the literature [13,54]. Factors that were found to determine privacy behavior include privacy concerns, privacy awareness, trust, demographics, and others. Additionally, previous research showed that some factors seem to affect privacy behavior more than others [13] while some factors affect privacy behavior directly or indirectly or with positive or negative way.

3. Theoretical Background

Experiential learning is an educational methodology that places significant emphasis on the value of acquiring knowledge through firsthand experiences, active involvement in practical tasks, and subsequent contemplation and analysis of those experiences [55]. The methodology suggests that individuals are more likely to gain knowledge, skills, and understanding in a more effective manner when they actively participate in and contemplate real-world events, as opposed to acquiring information passively inside the confines of a conventional classroom environment. Many researchers from the past until very recently claim that experiential learning is more advantageous than a traditional didactic approach [56–65]. According to Kolb [55] and Rogers [59], for a person to learn through experience, the following factors must be present:

- The participants must have the will to learn through the experience they lived;
- The participants should be able to reproduce the experience;
- The participants must have analytical thinking and understand the experience;
- The participants have the ability to make decisions and solve problems to create new ideas through the experiences they lived.

In addition, Boud [66] identifies the below three stages of the reflective process in the context of experiential learning and recognizes that this is a transformative process and the subjects can acquire new tendencies and abilities:

- The participant reviews the events and has the ability to study the experience again, calling this review a return to the experience;
- The participant recognizes the importance of the experience to third parties, through emotions;
- The participant discovers the new dimensions of the experience so that, through it, the change in his behavior occurs and creates a new way of thinking and new abilities.

Researchers from a wide array of scientific domains, such as psychology, sociology, philosophy, and health sciences, have embarked on extensive investigations to explore the intricacies of behavior and experiential learning. Their studies have encompassed various experiential learning strategies, which have provided valuable insights into how individuals acquire knowledge and skills through direct experience. These studies have typically employed various experiential learning approaches, encompassing visual and audio stimuli such as the ringing of a bell (term in psychology classical conditioning), practical assessments (term in psychology operant conditioning), and motivational interviewing.

3.1. Neural and Neutral Stimulation

Neural stimulation, in the context of neuroscience and physiology, refers to the process of applying a stimulus to excite or activate neural tissue (neurons) in the nervous system [67]. The utilization of this form of stimulation is frequently employed in scientific investigations to examine neurological processes, explore the impacts of particular stimuli on neurons, or as a therapeutic modality within the domains of neurology and psychiatry. Neural stimulation encompasses various techniques, including electrical stimulation, magnetic stimulation, and optogenetics (neutral stimulation). The latter use light as a

means to activate genetically modified neurons [67]. Numerous empirical studies have been undertaken in the field of psychology pertaining to the phenomenon of behavior transformation. Pavlov's classical conditioning experiment is widely recognized as one of the most renowned experiments in the field [68]. Through his empirical investigations involving canines, the researcher successfully established a conditioned response in the subjects by pairing a neutral stimulus, namely a bell, with the presentation of food. Consequently, the dogs exhibited salivation alone in reaction to the bell, devoid of any food-related stimuli. Bandura conducted an additional behavioral trial [69]. In his research, commonly referred to as "the Bobo Doll experiment", Bandura [69] demonstrated that youngsters who observed an adult engaging in hostile conduct towards the doll were more inclined to replicate the same aggressive behavior. Through this experiment, the researcher elucidated the notion of observational learning and its role in acquiring behavior through the process of observing others. Ainsworth's study [70] on attachment styles in infants explored the manner in which infants reacted to separations and reunions with their careers within the framework of the same theoretical construct. This experiment facilitated the comprehension of how various parenting behaviors might influence the behavioral style of a child. The results highlighted the importance of a stable bond between newborns and caregivers in promoting positive emotional growth. In a separate study, Watson and Rayner [71] conducted an experiment to illustrate the potential of an auditory stimulus, specifically a terrifying noise, as a catalyst for behavioral modification. Their findings emphasize the capacity for behavioral change through environmental stimuli. Asch experiment [72] additionally employed an optical manipulation to alter the observed behavior of participants. The study aimed to examine the degree to which individuals would comply to the opinion of a group, even when it contradicted their own personal judgment. The study involved the presentation of a basic perceptual task to the participants, which required them to assess line lengths. The participants were situated in an environment where they were exposed to confederates who intentionally provided inaccurate responses. The findings unveiled the significant impact of social conformity on individual decision making, providing insight into the intricacies of human behavior in social settings. In the same context, Becker's [73] research delved into the labeling theory, which posits that individuals tend to engage in deviant behavior when they are officially or socially classified as deviant by authorities or society. This particular viewpoint centers on the influence of social reactions on human conduct.

3.2. Practical Assessments

Practical assessments encompass evaluation methodologies or exercises that necessitate individuals to exhibit their knowledge, skills, and competences through tangible tasks, real-life applications, or hands-on activities. The purpose of these assessments is to evaluate an individual's capacity to apply theoretical knowledge in real-world scenarios, effectively solve issues, and successfully execute tasks that are pertinent to a specific field or subject [74]. Numerous strategies have been suggested within the realm of Information and Communication Technology (ICT) to alter privacy-related behaviors. These approaches encompass gamification techniques, privacy quizzes [75], and privacy simulators [76,77]. Practical evaluations adhere to Aristotle's renowned statement, which posits that the acquisition of skills is achieved via the active engagement in the respective activities. The concept of gamification for privacy behavior entails the incorporation of game-like components, such as incentives, obstacles, and rivalry, with the aim of motivating individuals to embrace and sustain privacy-oriented conduct in their digital engagements and online undertakings [75]. The process entails the utilization of game design principles to effectively engage and inspire users in making well-informed decisions pertaining to the safeguarding of their personal information, cybersecurity procedures, and compliance with privacy rules and regulations. In recent years, numerous approaches have been proposed or adopted. Mavroidi et al. [78] assert the possibility of gamification as a means to safeguard user privacy. The authors posit that the implementation of gamification holds

potential in the realm of privacy education, as it may effectively inform users about privacy concerns, motivate them to adopt privacy-conscious behaviors, and enhance the appeal of privacy-protective features. In a separate instance, scholars conducted a study examining the utilization of game-based learning (GBL) in the context of information security (IS) and privacy education and awareness [79]. The authors suggest that game-based learning (GBL) possesses the capacity to serve as a viable method for instructing information systems (IS) and privacy principles, owing to its ability to captivate learners, foster interactivity, and stimulate motivation. Respectively, the work of Drozd and Kirrane also supported these evidences [80]. In a separate study, the authors assert that game-based learning is a proficient method for educating individuals in technological domains, while also providing ample learning prospects for diverse target populations. The researchers asserted that the utilization of gamification in virtual reality escape rooms has the potential to enhance users' awareness of privacy matters [81]. On the contrary, gamification can also be utilized for evil purposes. Several studies suggest that the implementation of gamification carries inherent risks to user privacy. These risks include the possible exploitation of users' privacy, unauthorized collection of personal data, and the tracking of their online activities without their explicit authorization [82]. In an additional study [83], researchers discovered that individuals utilizing gamified services have a higher propensity to disclose personal information compared to those utilizing non-gamified services. The authors believe that the reason behind this phenomenon is the potential for gamification to induce cognitive absorption, thereby hindering users' capacity to make logical judgments regarding privacy.

Additional strategies that have been employed to alter privacy-related behaviors include the utilization of privacy simulators and privacy quizzes. Privacy simulators are software tools or systems that have been specifically designed to replicate and represent different facets of data privacy. These simulators are commonly used for teaching, testing, or research reasons. Simulators are utilized to generate synthetic data or scenarios that replicate real-world privacy difficulties, enabling users to enhance their comprehension and assessment of privacy threats, compliance with data protection legislation, and the efficacy of privacy-enhancing methods. As an illustration, Bum et al. [76] devised a simulator aimed at enhancing individuals' awareness of privacy matters and facilitating their comprehension of the privacy consequences associated with their online behaviors. In a separate study, the researchers developed a simulator for mobile security and privacy. This simulator allows for the simulation of mobile entities and their surrounding environment, facilitating the investigation of security and privacy concerns [84]. The authors asserted that simulation can be employed to assess privacy dangers and countermeasures using numerical analysis and visualization, enabling a more comprehensive understanding of the ramifications and privacy threats faced by users. Privacy quizzes are interactive evaluations or surveys created to check an individual's comprehension and familiarity with concepts, principles, legislation, and optimal approaches pertaining to privacy. The quizzes commonly have a range of question formats, including multiple choice, true/false, and open ended, which encompass diverse dimensions of data privacy and security. Privacy quizzes are frequently employed as pedagogical instruments, instructional modules, or consciousness-raising initiatives to enable individuals and entities to assess their proficiency in matters of privacy and discern domains that necessitate enhancement. In their study, Leenen and van Vuuren [75] asserted that privacy quizzes serve as a means to encourage secure online conduct and represent an efficient and cost-effective approach in aiding the military community in the prevention and detection of online threats.

3.3. Motivational Interviewing

Motivational interviewing (MI) is a counseling technique and communication method that prioritizes assisting individuals in examining and resolving their conflicting feelings regarding modifying their behavior. This approach demonstrates notable efficacy within circumstances characterized by people who exhibit resistance or reluctance to modify their behaviors, such as addiction treatment, health care, and mental health counseling.

Motivational interviewing (MI) is a therapeutic approach that encompasses the utilization of active listening, empathy, and non-confrontational questioning techniques. These strategies are employed to facilitate individuals in recognizing their own motives and aspirations for personal transformation, hence enhancing their preparedness to initiate behavioral change [85]. Motivational interviewing (MI) can be integrated with other behavioral modification techniques, such as cognitive behavioral therapy (CBT), in order to enhance the efficacy of interventions aimed at promoting behavior change [86]. The aforementioned methodologies are commonly employed in the disciplines of psychology and sociology to effectively tackle a range of behavioral issues, including but not limited to anxiety disorders and eating disorders [86]. Recently, there has been an emergence of a novel variant of cognitive behavioral therapy known as cognitive behavioral transformation (CBTx), which has begun to be employed in practice. Cognitive behavioral therapy (CBT) places emphasis on facilitating individuals in the process of modifying their fundamental beliefs and assumptions. CBTx operates under the premise that our fundamental ideas and assumptions regarding ourselves, the world, and others exert a significant influence on our cognitive processes, emotional experiences, and behavioral patterns. The existing body of literature on CBTx is still minimal. However, certain tests undertaken with CBTx have reported positive outcomes in terms of attitude, well-being, and learning [87–89].

3.4. The Research Method

As we demonstrated in this section, experiential methods offer more benefits than traditional learning and education [55–58]. Based on the fact that the cognitive model was created by the field of psychology, this field considers the monitoring of the individual's phlegmatic response such as facial expressions and emotion recognition and the recording of the individual's personal narratives to be extremely essential [90]. A person who is able to verbally or physically convey an emotion may have trouble expressing it in writing or require assistance or a reward from the researcher [91,92]. At this juncture, the researcher records both the participant's possible written or verbal response to a question as well as their physical reaction. This response may be identical to the participant's or completely different. During the literature review of the fields of the sciences of psychology, philosophy, and sociology, the methods that were followed by the vast majority were field research and analysis based on qualitative methods, as each individual may exhibit a completely different behavior than another individual despite having the same or similar characteristics [55–57,61–64]. Numerous factors, such as socio-cultural approaches, social milieu, previous experiences, and economic status, can influence a person's behavior, so demographic characteristics are not the only focus in the field of psychology. We chose the qualitative research methodology for the aforementioned reasons and because the premise of the experiment is the proof of experiential methods of learning and education against the dominant model.

4. The Proposed Experiential Privacy Behavior Transformation Framework

Section 3 has elucidated that behavior can be modified by many methods and stimuli. In the realm of psychological experimentation, researchers frequently employ neutral stimuli, such as noises and visual effects. Conversely, within the fields of sociology, health, and psychology, motivational interviews are commonly utilized in conjunction with cognitive behavioral therapy (CBT) and CBT-based theories. In contrast, within the field of information technology, practical methods such as practical assessments and gamification approaches are predominantly employed for the purpose of transforming privacy behavior. In this section, we present our framework for transforming privacy behavior, based on the literature review and the theoretical background presented above.

As stated in the literature review, prior studies have endeavored to consolidate the factors that are mentioned in the existing literature as determinants of privacy behavior [13,54]. In these works, the researchers examined the relationship between determinant elements of privacy behavior, such as fear and financial-non financial exchanges, and the influential

axes of the cognitive theory, namely beliefs, perceptions, and attributions. Further, as described in Section 3, experiential learning approaches include visual and audio stimuli, practical assessments and motivational interviewing. Therefore, our framework will encompass neutral stimuli, practical assessments and motivational interviewing with regard to their efficiency to transform individuals' privacy behavior.

We define two types of neutral stimuli, namely short-length visual content and long-length visual content regarding privacy behavior. We define three types of practical evaluations: (a) privacy behavior quizzes, (b) privacy behavior simulators, and (c) privacy behavior gamification methods. We consider motivational interviews to assess privacy outcomes related to meta-data mobile phone monitoring and google account monitoring from the side of privacy-related incidents. The aforementioned concepts are depicted in Figure 1.

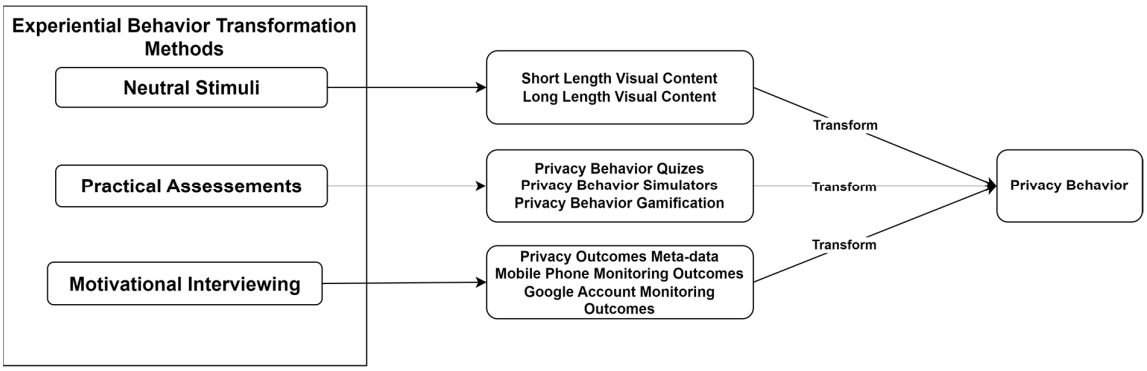

Figure 1. Experiential privacy behavior transformation framework.

Due to the fact that in addition to experientialism, our model also incorporates training on increasing the perception of risks and questions on the results of our experiment's questions, a qualitative method rather than a quantitative one was chosen for the experiment. The experimental design is also a consideration when selecting a qualitative technique. Due to the fact that the individuals will be monitored with our own apparatus, it was necessary to have physical access to them. In a later phase of the experiment, each participant will undergo an interview and training phase at the same time as they progress through the experience's stages.

For the design of the empirical research, we will adopt observation and behavior techniques witnessed in psychology and sociology. As mentioned in Section 3, these techniques are conducted qualitatively by employing narrative interviews and field research. The primary reason for this choice is that the researcher aims to observe the participant's reaction and response. In relevant empirical studies, the researcher places participants in dilemma situations and observes the initial reaction to chain questions and how behavior changes over time.

5. Methodology to Empirically Test the Proposed Framework

In this section, we present the validation methodology of our framework, which comprises five phases. We describe and analyze every phase of the methodology to validate the proposed behavioral transformation framework, including the respective scope and target per phase.

We adopted a multiple stratification methodology to empirically test our proposed framework. As demonstrated in Paspatis et al. [13], privacy behavior is influenced by a variety of factors. Similarly, Paspatis and Tsohou [54] show that the cognitive processes of privacy behavior are influenced by three cognitive axes of influence, with each axis being influenced by a distinct set of factors, which are sometimes present in two or three axes.

Our methodology to test our framework is divided into five phases as described below:

- Phase 1: Creation of qualitative questionnaire with multiple-choice and open-type questions to assess users' privacy behavior.
- Phase 2: Implementation of privacy behavior measurement using the methods derived from phase 1 in a small, closed group of up to 10 individuals.
- Phase 3: Creation of the experimental environment per experiential method (i.e., neutral stimuli, practical assessments, motivational interviews).
- Phase 4: Implementation of the experiential experiment aiming towards privacy behavior transformation.
- Phase 5: Analysis of results with regard to the success of behavioral transformation.

The above phases are illustrated in the figure below (Figure 2).

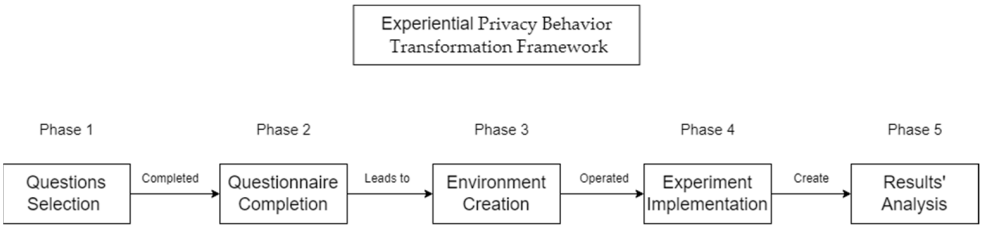

Figure 2. Capture of experimental phases.

5.1. Participants' Selection Criteria and Profile

People from our broader social milieu and outside our sphere of influence were chosen for the experiment. In order to enlist the volunteers, we conducted a thorough search throughout our wider surroundings. The selection criteria primarily consisted of three factors: unfamiliarity with the participants to prevent any bias, no personal connections such as family, academic affiliation, or university enrollment to maintain impartiality, and being an adult to meet the requirements for signing the consent form to participate in the experiment. The majority of the participants were recruited using the "friends of a friend" tactic. Individuals were selected using a stratified method. Specifically, we selected participants from as wide a range of age, gender, educational level, and occupation. We made a deliberate effort to ensure an equal representation of both genders, with participants having varied occupations. Additionally, each participant had a minimum age difference of 5 years from others, regardless of gender. The objective of the stratification method was to assess the effectiveness of the framework in all conceivable combinations. Although more than 20 individuals initially expressed interest, some withdrew due to privacy concerns after receiving additional information. When we informed the participants about the duration of the experiment and the amount of effort required, some of them revoke their willingness to participate.

Every participant signed an analytical consent form in order to engage in the study. In addition to the consent form, all participants received additional information regarding the experiment, which may not have been extensively covered in the consent form. This information included an analytical overview of the experiment as well as any anticipated advantages for the participants, researchers, and society. The consent form and the experiment adhered to the ethical standards of our institution and followed Cope's best practices [93]. Initial interest was expressed by 22 individuals, 9 women and 13 males. After withdrawals and exclusions, four women and five men were ultimately chosen. The participants' age ranged from 26 to 62, with a mean of 40.89 years, a median of 36 years, and a standard deviation of 11.33 years. Despite the large age range of 26 to 62 years, the sample's mean value was relatively close to the sample's mean, as indicated by the standard deviation. We can conclude from the above that our sample is representative of this value range. Four people had a university education, two women and two men, of which two had a master's degree; three people had a technological education, two women and one man, of which two had a master's degree; and two people had a complete secondary education, one woman and one man, of which one has a qualification. Three participants held bache-

lor's or master's degrees in information technology. Participants' profile is presented in Table 1.

Table 1. Profile of participants.

Participant Number	Index	Gender	Age	Education	Occupation
Participant 1	CD	W	47	University Education	Philologist
Participant 2	PE	M	36	University Education	Police officer
Participant 3	NB	M	46	University Education	Military
Participant 4	DS	W	50	University Education	IT
Participant 5	PM	M	62	University Education	Refrigerant
Participant 6	PW	W	36	Technological Education	Technologist
Participant 7	AA	M	36	Technological Education	Technologist
Participant 8	AE	W	29	High School	Employee
Participant 9	TE	M	26	High School	Employee
Total: 9		AVG = 40.9 y		MD = 36 y	SD = 11.33

5.2. Phase 1. Creation of Qualitative Questionnaire to Assess Users' Privacy Behavior

In this phase, a qualitative questionnaire was created to assess participants' current privacy behavior. The purpose of this questionnaire is to assess the current (pre-study) privacy behavior of the participants who will be involved in the experiment. The participants were asked to complete again the same questionnaire after the experimental process, so that we can compare the pre- and post-evaluations. The questions of the questionnaire are presented as Appendix A.

Each question was selected after comprehensive research in academic journals such as the basket of eight and google scholar search engines. The questionnaire inquiries were derived from a collection of articles on privacy-related behavior. Regarding the questionnaire, each question may appear in more than one of the selected questionnaires. Each question may not be presented verbatim, but its core meaning or purpose remains the same as other questions with similar wording. In addition, each question was selected so that it could be used as a variable in our conceptual model for further analysis, while also being associated with at least one of the influencing factors of privacy behavior identified in our previous research [13]. Additionally, each selected question was modified to be asked as open question due to our qualitative process but it is also could be rated on a 5-point Likert scale ranging from "Very often" to "rarely". Thus, if a question was in 7-point Likert form then the two extreme values on a 7-point Likert scale were merged with the preceding value. For instance, "Too often" and "Very often" have been merged into "Very often".

Further, we matched each question with at least one influencing factor of privacy behavior as they emerged from the work of Paspatis et al. [13]. For the sake of convenience each factor matched to an acronym as they are appearing to Table 2. As matching criteria, we used the "nearest neighbor" methodology as they emerged from our previous research [54]. The nearest neighbor matching method is especially advantageous when the number of variables is limited. This method is applicable in various domains including as epidemiology, economics, and psychology. It is used to assess the similarities between observed variables, the close correlations among observed variables, or the outcome of a statistical or medical experiment [94].

Table 2 demonstrates the acronyms of the affected factor or cluster of factors while Table 3 demonstrates the questions and the number of articles addressing these as well as the affected factor(s).

Table 2. Privacy behavior factors obtained by Paspatis et al. [13].

Factor or Cluster	Acronym
Financial Exchanges/Benefits/Usefulness	FEBU
Privacy Risk Perception	PRP
Trust/Control/Confidence/Fear	TCCF
Privacy Concerns	PC
"Needs"/Psychological Engagement/Necessity	NPEN
Sensitivity of Information	SOI
Privacy Awareness	PA
Time Lapse	TL
Education/Visualization/Interaction/Experience	EVIE
Demographics	DE
Dimensionality/Complexity of Privacy Decision Making	DC

Table 3. Questionnaire to assess users' privacy behavior.

Activated Factor	Question	Number of Articles
PA	Q1: How often do you check the privacy settings on your social media accounts?	5
TCCF, PRP, PC	Q2: How often you felt like your privacy was violated online?	5
PA	Q3: How often do you read the privacy policies or terms of service for the websites or apps you use?	5
PA, PC	Q4: Have you ever declined to use a service or app because of privacy concerns? If so, can you describe the situation (open)?	5
PA, PC	Q5: How often do you use different passwords for different accounts? How do you keep track of them (open)?	4
TCFF	Q6: Have you ever been a victim of identity theft or online fraud? How did that experience affect your privacy behaviors (open)?	4
PRP, PA	Q7: How much personal information do you share online? Can you describe the reason (open)?	5
PA	Q8: How often do you take steps to protect your online privacy? Do you use ad-blockers or other tools and which (open)?	4
PRP, TCFF	Q9: Did you know companies collecting and using your personal data for targeted advertising?	5
PC	Q10: Do you have any concerns about government surveillance or monitoring of your online activities?	3

5.3. Phase 2. Implementation of Privacy Behavior Measurement

To conduct the qualitative questionnaire, we used mixed methods. Due to some participants' educational level and/or computer skills familiarity, four of the questionnaires were completed with the help of the researcher during a physical meeting; in most cases, when this was not possible due to distance or time limitations, the meeting was conducted online. Prior to distributing the questionnaire, we notified the participants that all their personal data and identifiers will be anonymized. The purpose of this option is to convince respondents that they cannot be identified so that they will answer the questions more truthfully. Murdoch [95] found that people who assume they cannot isolate themselves from the results of a survey are approximately nine percent more likely to participate and to provide the most accurate response possible. Thus, for the same reason, we did not reveal how many people participated.

5.4. Phase 3. Creation of the Experimental Environment Per Experiential Method

We devoted great effort to create an experimental environment to cover both our specifications and also create a nice and full anonymized experience for the participants of the experiment. We emphasized making the participants feel comfortable and secure about their privacy and their personal data. We were also transparent with our methodology to mitigate any of their privacy concerns. Due to page limitations, we will not go into detail about our infrastructure. In summary, our experimental environment consists of the following key components:

- One central and nine client Gmail accounts (IonianUniversityLab@gmail.com, ionianuniversitylabvictim1-9@gmail.com);
- Virtual machines;
- Multiple streaming platform accounts in a legal, secure and anonymized way;
- Other applications (e.g., Family Link, Viber, and Streaming Platform App).

The Gmail accounts were used with the build-in app "find my device" and were remotely installed in participants' phones (more information to the next subsection) along with other necessary applications such as family link and Viber. To establish a secure, anonymous, and legally compliant visual content environment, we implemented a privacy protocol that incorporates several levels to enhance privacy. These layers include a VPN browser plugin, temporary email services, and crypto-cards. The aforementioned approach was implemented to guarantee anonymity for both us and the participants. Conversely, the goal of the streaming platform service is to offer a lawful means for our participants to access the privacy-related content we selected. The multi-layer anonymity procedure we followed is pictured to the following Figure 3.

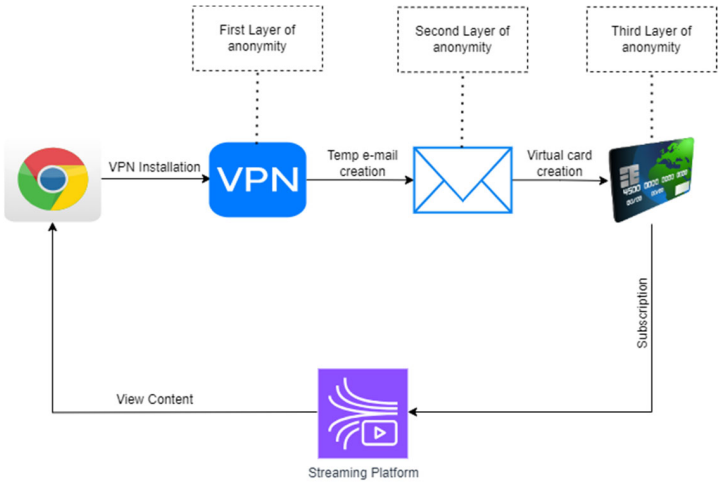

Figure 3. The multi-layer anonymity procedure.

5.5. Phase 4. Implementation of the Experiential Experiment Aiming towards Privacy Behavior Transformation

As we analyzed in Sections 3 and 4, privacy behavior can be transformed mainly using three methods (content viewing, practical assessments and one-to-one motivational interviews), with neutral or visual stimulus, by practicing and by external motivation speeches such as motivational interviews. In our experiment, we included all three methods in order to test our framework.

In the following, we describe the three experiential procedures that we followed. During the experimental period, we gave the participants a two-sim card mobile android phone. The participants used the one sim slot for the sim card that belong to us and the second sim slot could be used for own sim card, if selected. We opted for this choice to avoid making them uncomfortable by carrying two smartphones (own and experiment) and because we expect that this would allow them to use the experimental phone to the

maximum. All participants were part of all three experiential procedures, content viewing, practical assessments and one-to-one motivational interview. We provide more details about the experimental procedures in Appendix C. Due to the lack of multiple experimental mobile devices and sim cards, we included the participants sequentially and not in parallel (so that the same phones could be used by several participants).

After the execution of two of the experiential procedures (content watching and practical assessments), we gathered all the information in order to construct the material for the motivational interview. Motivational interviewing is our final part of the experiential methods that the participants took part in.

5.6. Phase 5. Results Analysis and Framework Validation

This phase includes the analysis of the experiment data to investigate if behavioral transformation was successful.

First, we re-executed the questionnaire of phase 1 and compared the data with that of phase 4, per participant, to assess if self-reported behavioral transformation was successful. In this step, we gathered the results of the first questionnaire and we compared them with their last answers in order to calculate if their privacy self-reported behavior changed and by how much. To calculate the difference, we weight the responses from the first and second questionnaires into 5-point Likert-type scores and perform two-stage ANOVAs [96] as well as Cronbach's A-tests [97].

Second, to assess participants' actual privacy behavior transformation, we re-monitored participants for a smaller period of 10 days. This way, we can collect information about actual privacy behavior and compare with the data that we collected during phase 4, so as to assess if actual privacy behavior was transformed. The decision to reduce the re-monitoring stage to a 10-day duration instead of 30 days was taken due to resource constraints. As previously stated in Section 5.5, multiple participants utilized the same mobile phones due to a scarcity of available experimental devices. In order to expedite the re-monitoring process, we decided to reduce the duration from 30 days to 10 days. The re-monitoring process was conducted utilizing identical procedures, tools and equipment to the initial 30-day period.

For the sake of completeness in Appendix C, we provide all the content and the items we used in our framework.

6. Results

This section provides the results of our empirical study.

6.1. Pre-Study Privacy Behavior Assessment

We utilized Google Forms to create and disseminate Appendix A. The selection was made based on the speed at which a form could be generated, the simplicity of distributing it, and the ease of processing the data. As previously stated, nine people participated. The questionnaire was distributed to our participants through various channels, including email, a hyperlink, and direct messages on the social media platforms Facebook (Meta) and Viber. Hence, we notified the participants that they are required to finalize the questionnaire within a period of 10 days. Participants who were unfamiliar with the Google Forms platform or lacked the necessary technological skills were provided assistance by scheduling an appointment with our team. At last, all nine participants successfully submitted the questionnaire.

The results were initially examined using a two-factor quantitative ANOVA approach without replication. We choose the ANOVA approach due to its recommendation for situations where there are several factors that influence an independent variable. As we have seen in Section 2, there are a total of eleven determining factors. Furthermore, ANOVA is suggested for assessing multiphase techniques, as we will perform in our specific situation. Cronbach's Alpha was utilized to assess the validity of the questionnaire. Due to the limited number of participants (n = 9), this approach was used as it is considered the most straightforward technique for testing a questionnaire. Furthermore, as the objective of

this questionnaire is not to extract or elucidate any phenomenon, but rather to compare the outcomes prior to and following the experiential transformation, we have concluded that more intricate quantitative analysis methodologies are unnecessary. However, the results are primarily presented for the sake of comprehensiveness and also for potential statistical analysis in the future, either by the current researchers or other scholars. Regarding the descriptive results, it was evident that all participants consistently exhibited risky privacy behavior across all questions, with an average score of 4.09. This suggests for example that privacy settings are seldom or rarely modified, or that the participants have a low level of privacy-conscious behavior. Table 4 presents the overall and individual question averages. Concerning the implementation of the ANOVA, it is evident that the participants' responses to each query do not exhibit a statistically significant disparity (F = 1.19, p-value = 0.31, p = 0.5), despite a considerable likelihood of inaccuracy. On the other hand, each person shows a pretty little difference for each question (F = 3.57 > F critical 2.07, p-value = 0.001, p = 0.05). The ANOVA analysis outcomes are presented in Table 5. Cronbach's application demonstrated a performance validity of 0.71961223 (Table 6). The questionnaire responses are considered adequate and reliable, as demonstrated in Tables 4–6.

Table 4. Participants' answers.

Participant	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Avg
Participant 1	5	5	4	5	5	5	5	4	5	5	4.80
Participant 2	4	5	4	5	4	4	5	4	5	4	4.40
Participant 3	5	5	4	5	5	5	5	4	5	5	4.80
Participant 4	2	4	4	5	4	2	4	4	5	4	3.80
Participant 5	5	4	4	5	3	5	4	4	5	3	4.20
Participant 6	5	3	3	5	5	5	3	3	5	5	4.20
Participant 7	4	3	5	4	4	4	3	5	4	4	4.00
Participant 8	4	5	2	4	3	4	5	2	4	3	3.60
Participant 9	3	5	1	1	5	3	5	1	1	5	3.00
Total Average	4.11	4.33	3.44	4.33	4.22	4.11	4.33	3.44	4.33	4.22	4.09

Table 5. ANOVA summary table.

ANOVA						
Source of Variation	**SS**	**df**	**MS**	**F**	***p*-Value**	**F-Crit**
Rows	26.48889	8	3.311111	3.566489	0.001557	2.069832
Columns	9.955556	9	1.106173	1.191489	0.313744	2.012705
Error	66.84444	72	0.928395			
Total	103.2889	89				

Table 6. Cronbach's Alpha internal consistency matrix.

Cronbach's Alpha	Internal Consistency
$0.9 \leq \alpha$	Excellent
$0.8 \leq \alpha < 0.9$	Good
$0.7 \leq \alpha < 0.8$	Acceptable
$0.6 \leq \alpha < 0.7$	Questionable
$0.5 \leq \alpha < 0.6$	Poor
$\alpha < 0.5$	Unacceptable
Participants' Score:	0.71961223

6.2. Monitoring Results

During the initial phase, participants were provided with a phone that was accepting two SIM cards simultaneously. As previously said, we closely observed the participants using various methods for a duration of 30 days. Throughout this duration, we effectively observed and tracked all individuals involved. To obtain the mobility and location data of each participant and effectively analyze them, we retrieved all the accessible information. To accomplish this, we initially attempted to utilize the Google Takeout service. However, we encountered various problematic issues, such as the inability to pick certain date and time ranges. To address the issue mentioned above, we employed a bespoke Python script that leveraged the cookies of the participants. Through the surveillance of Viber's desktop sqlite database, in conjunction with findmydevice, we have effectively obtained data on participants' daily routines, including their place of residence, workplace, preferred WiFi hotspots, and real-time position tracking. We effectively utilized the GPX file data from sports apps like Strava and Endomondo to extract information about participants' hobbies, preferred sports locations, and GPS data. It should be noted that GPX file data are accessible to anybody on the mentioned platforms, provided that the platform user has not protected it by modifying the privacy settings. It is important to note that none of the participants chose to uninstall any pre-installed applications, despite being informed of their ability to do so. We will utilize some of the aforementioned processed data as proof and as a means to enhance awareness during the motivational interviews in the experiential procedure 3.

6.3. Experiential Procedures

6.3.1. Experiential Procedure 1. Content Viewing

Throughout the phone-monitoring period, all participants were required to access the privacy behavior content that we had provided on the chosen streaming platform and other media platforms. In order to ensure the viewing of content, we closely watched the content history area of each platform. Based on the information provided, we can confirm that all participants were exposed to the instructed content. However, it is not possible to verify this with certainty, as the participants may have initiated the media content and subsequently discontinued their engagement. In order to enhance obedience, we incorporated additional content-related questions into the motivational interviewing process.

6.3.2. Experiential Procedure 2. Practical Assessments

At this point, the participants were required to select and utilize at least one item from each category, including privacy-related tests, privacy emulators, and privacy-related games. In addition, they were required to upload a minimum of one photograph to their chosen social media platform. In order to assure compliance, the participants were required to provide their personal scores for each practical assessment tool they selected. Each participant could select multiple tools from each category, but just one tool should be chosen as the minimum requirement. The privacy-related meta-data, if available, will be utilized in the motivational interviewing procedure. The time frame to complete all of the aforementioned tasks was identical to the previously mentioned 30-day period.

6.3.3. Experiential Procedure 3. Motivational Interviews

In this section, we initially provided our monitoring findings to each participant individually, as indicated in Section 4. The objective of this activity is to demonstrate the extent of personal information that may be obtained by an application developer, company, or individual using a seemingly harmless program, such as a free flashlight app from a marketplace. By presenting individuals with the data collected by monitoring their phone activities, we aimed to trigger the most influential causes for behavioral change, such as fear and concerns about privacy. As stated in the literature review section, if we elicit the instinct of fear in humans by visual stimuli, it will lead to a significant and lasting change in their behavior. Following their findings presentation, the procedure proceeds with a qualitative and open-ended questionnaire designed to provide further insight into their emotional

state regarding their privacy. The objective of this questionnaire is to ascertain individuals' perspectives on their emotions over the disclosure of personal information and whether they require or desire our assistance in safeguarding it. For example, Question 3 asks (we): "Did you know that a service or an app such as google timeline could monitor your daily movement? How you feel about it? That lead to the answer: Participant PE: "Firstly, I never knew the existence of this app. Firstly, I heard about it through this experiment. I felt like a victim of monitoring of some company. The details about my daily movement such as going to get by girls from daycare scared me about my safety and the safety of my family" Question (we): What would you like to do? PE: "Can I disable this function? If I disable it my phone will continue to be functional?" (We): "Sure you can deactivate it. Let me show it to you". The protocol of the motivational theory stipulates that, in this final phase, all inquiries or responses to the participant should be presented in a positive manner, without judgment or negativity. The questions of the motivational interviewing technique are presented in Appendix B. The questions, as well as the subsequent follow-up questions, can vary depending on the participant's answers and subsequent inquiries.

6.4. Questionnaire Re-Execution

In order to assess any potential changes in participants' self-reported privacy behavior, we requested them to once again complete the phase-2 questionnaire (Appendix A). The objective of this action was to obtain the updated values following the completion of all the experimental procedures. Following this phase, the two questionnaires were compared using two different methods. Firstly, through descriptive analysis, we analyze and process the averages of each question individually. We conducted a comparative analysis of each participant's responses, both on a question-by-question basis and in terms of the overall average. Furthermore, we employed a paired T-test on each item to determine the statistical significance of the observed differences. Based on the findings, we may deduce that the self-reported privacy behavior of each participant has shown improvement in nearly all of the questions. The *t*-tests we conducted demonstrated that the *p*-values for each question were significantly below 0.05, indicating a substantial and meaningful change in behavior. Therefore, it is important to note that participants with higher levels of education had lower changes in behavior. Additionally, it is possible that having a degree in the IT field influenced the results. Due to the limited size of the group, it is difficult to determine with certainty if a degree, particularly in IT, had a significant impact on the observed behavioral changes. The table below displays the participants' replies to Appendix A, together with the *p*-value obtained from the T-test conducted comparing the two questionnaires. Table 7 below displays the outcomes of the questionnaire that was re-administered.

Table 7. Participants' answers on Appendix A re-execution.

Part/Ant	Q′1	Q′2	Q′3	Q′4	Q′5	Q′6	Q′7	Q′8	Q′9	Q′10
Participant 1	3	3	4	4	3	3	3	3	4	3
Participant 2	2	3	3	4	3	3	3	3	4	3
Participant 3	2	2	4	2	3	3	3	3	3	3
Participant 4	2	2	3	2	2	2	4	4	3	3
Participant 5	3	2	3	4	2	3	3	3	3	2
Participant 6	2	2	2	3	2	2	3	3	4	3
Participant 7	2	2	3	2	1	2	2	3	4	3
Participant 8	1	2	2	2	3	2	3	2	3	2
Participant 9	1	5	1	1	2	2	3	1	1	2
p-value	0.00013	0.00058	0.02220	0.00105	0.00066	0.00042	0.00171	0.02220	0.00275	0.00020

6.5. Framework Validation (Monitoring Re-Execution)

Shortly after concluding the experiential techniques, we requested the participants to undergo mobile monitoring, similar to phase-2, but for a duration of 10 days. The objective of this action was to verify the effectiveness of our framework, not only through participants' self-reported privacy behavior, but also through their actual privacy behavior. Once again, the participants did not receive the phone and the SIM card simultaneously due to the limited availability of phones and SIM cards. As a result, several individuals received the equipment a few days after their prior monitoring, while others had to wait for a longer duration, up to 4 months after the experimental procedures concluded. Initially, we were concerned that some participants could revert to their previous privacy-related behaviors, but this did not actually occur. Out of the nine participants, six of them disabled location permissions for most of the apps, including Google services and Viber. Among these six participants, two of them specifically inquired about how to disable these permissions. Out of the nine participants, eight uninstalled the lens application that we had previously installed and had both location and actual location rights enabled. All individuals refrained from posting any images on the social networks they utilized during the initial monitoring period. Ultimately, none of the participants were able to successfully uninstall the family connection app, likely due to the software's intentional design to resist removal and the requirement of sophisticated technical expertise for such an activity.

6.6. Final Results

Based on the information provided, we conclude that the experiment was successful for most of the participants. The privacy behavior of all participants appears to have undergone a significant transformation towards increased privacy protection, at least from the conclusion of the experimental procedures until a period of four months thereafter, answering research question 1. Not all participants exhibited the same level of transformation in their privacy behavior, and we are now unable to provide a complete explanation for this phenomenon. Furthermore, we did not anticipate this outcome. Several factors can influence the extent to which participants' privacy behavior changes, including their demographic background and their level of IT education. We deliberately selected participants spanning a wide age range (26–62 years old) and varying educational levels, ranging from high school to individuals with a master's degree, to assess the effectiveness of the framework in transforming privacy behavior regardless of one's academic background. Based on the conversations in the motivating interview and the qualitative questionnaire responses (open-ended answers), we have determined that participants found visual stimulations (experiential procedure 1) to be more effective in transforming their privacy behavior, answering research question 2. Consistently, participants indicated that their monitored findings, along with the motivating interview's positive discourse, aided their comprehension of their prior privacy behavior level. The majority of the participants regarded the results of procedure 3 to be enlightening. However, without external assistance, it would be challenging for them to initially recognize the extent of their personal information exposure and the necessary precautions they should take to safeguard themselves. Ultimately, participants deemed the practical assessments to be beneficial although occasionally tedious. They provided assistance in determining their present level of privacy and recommended changes to enhance their protection, albeit in a less inspiring manner compared to the other two procedures.

7. Conclusions

The investigation of individuals' privacy behavior and their corresponding activities has been a phenomenon that we have been studying for over 20 years. However, in academia, the prevailing methods to shape an individual's private behavior primarily consist of conventional teaching approaches, despite the fact that most people still rely on this method for learning or may not receive any education on this issue at all. Our research did not uncover any evidence of a privacy behavior transformation framework being used

in primary or high schools. However, such frameworks are predominantly found in higher education, particularly in academic syllabi that are IT focused. In contrast, disciplines like sociology and psychology have extensively conducted research and experiments to modify individuals' behavior.

The integrated privacy behavior transformation framework we propose draws upon theories and experiences from the disciplines listed above. By leveraging our prior research on factors influencing privacy behavior and conducting an extensive literature analysis on behavior modification theories in other domains, we have successfully crafted a robust framework for transforming privacy behavior. To assess and confirm the effectiveness of our framework, we carried out a controlled experiment, which provided validation for our framework. To the best of our knowledge, this is the initial comprehensive framework that aims to modify an individual's privacy behavior using proven experiential methods.

This framework could prove advantageous to the academic community by facilitating the learning of privacy behavior alteration from individuals' early age and continuing even after they have completed their educational journey. Our framework can be utilized by elementary schools, academic institutes, and private schools to enhance students' adherence to protective privacy behavior. Furthermore, it has the potential to redirect the focus of privacy scholars onto novel avenues of investigation.

The scope of our findings regarding the changing of privacy behavior by experiential aspects is restricted. The experiment was conducted with restricted resources and within a small group of individuals. Hence, our objective is to enhance our framework by identifying its vulnerabilities and subsequently refining them. Our future research will focus on evaluating our framework in more detail and detail and with a larger group of participants, exploring improved approaches to promote individuals' privacy behavior while reducing our intrusion. This includes investigating alternate methods to phone surveillance that we previously employed by a less privacy-intrusive one.

Author Contributions: Conceptualization, I.P. and A.T.; methodology I.P.; formal analysis, A.T.; investigation, I.P.; writing—original draft preparation, I.P.; writing—review and editing, I.P. and A.T.; visualization, I.P.; supervision, A.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to prior informed consent of the par-ticipants before the start of the study as well as the provided declaration form of the authors that COPE guidelines were followed during conducting this research. Informed consent was obtained from all subjects involved in the study.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data is unavailable due to privacy restrictions.

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

Appendix A. Questionnaire (ENG)

1. [PA] How often do you check the privacy settings on your social media accounts?
2. [TCCF,PRP,PC] How often you felt like your privacy was violated online?
3. [PA] How often do you read the privacy policies or terms of service for the websites or apps you use?
4. [PA,PC] Have you ever declined to use a service or app because of privacy concerns? If so, can you describe the situation (open)?
5. [PA,PC] Do you use different passwords for different accounts? How do you keep track of them (open)?
6. [TCFF] Have you ever been a victim of identity theft or online fraud? How did that experience affect your privacy behaviors (open)?
7. [PRP,PA] How much personal information do you share online? Can you describe the reason (open)?

8. [PA] How often do you take steps to protect your online privacy? Do you use ad-blockers or other tools and which (open)?
9. [PRP,TCFF] Did you know companies collecting and using your personal data for targeted advertising?
10. [PC] Do you have any concerns about government surveillance or monitoring of your online activities?

Appendix B. English (Interview Questions)

Questions based on experiment (Likert 1–5) of qualitative.

(1) [TCCF, PC, PA, EVIE] Interview and simultaneous demonstration of her/her personalized image as well as data we have recovered, habits, etc. How do you feel about this?
(2) [PA, PC, EVIE] Did you know that a lens app could access your daily location?
(3) [TCCF, PC, PA, EVE] How do you feel about this? H8b triggering fear, privacy risk concerns, privacy awareness through visualization

Did you know that automatically or automatically someone or a company could create your daily patterns such as waking up in the morning, what you go to or leave your job, or when and where you train?

(1) [PA, TCCF] How do you feel about this?
(2) [PA, PRP] Did you know that through your posted photos you could find the time and place they were taken or other data?
(3) [TCCF, PRP, PC] How do you feel about it?
(4) [PA, PRP] Do you think you should disable Google timeline, Strava, Viber? (photo from Viber/sqlite/Strava)
(5) [EVIE] Will you do it or will you ask for help with it?
(6) [EVIE] Do you know how to remove permissions from apps?
(7) [PA, PC, PRP] Will you search and remove permissions from apps?
(8) [PA, PC, PRP Will you continue to post photos on social networks?
(9) [PA, PC, PRP Do you feel upset that a company or even a developer can create patterns of your daily life?

Appendix C. Experiment Content and Items

Table A1. Visual content and stimulations.

Activated Factor(s)	Movie/Series Name	Short Description	Purpose and Target
PRP, TCCF, PA, EVIE	The Great Hack	The Cambridge Analytica scandal is examined through the roles of several affected persons.	Awareness of the handling of personal data by social platforms. Decreased trust in social networks.
PRP, TTCF, PA, EVIE	The Social Dilemma	Explores the dangerous human impact of social networking, with tech experts sounding the alarm on their own creations.	Awareness of the handling of personal data by social platforms. Decreased trust in social networks.
FEBU, TCCF, NPEN, EVIE	Black Mirror: Nosedive	A woman desperate to boost her social media score hits the jackpot when she's invited to a swanky wedding, but the trip doesn't go as planned.	Social media awareness. Indication of compulsive behavior.
TCCF, NPEN, PA, TL	Black Mirror: Smithereens	A cab driver with an agenda becomes the centre of attention on a day that rapidly spirals out of control.	Awareness of social networks and risks of compulsive behavior.

Table A2. Short videos items.

Activated Factor(s)	Video Name	Short Description	Purpose and Target
PA, EVIE	"How to Protect Your Privacy Online" by Techquickie	This video covers the basics of online privacy and offers practical tips for staying safe on the internet.	Social media privacy awareness enhancer.
PA, TCCF, PC, EVIE	Data Protection and Privacy.	(animated). Increasingly, an ever-wider range of economic, political and social activities are moving online, encompassing various kinds of information and communications technologies (ICTs). The evolving ICT use is having a transformational impact on the way business is done, and the way people interact among themselves, as well as with government, enterprises and other stakeholders.	Personal data protection privacy awareness, data control enhancer regarding companies, government, etc.
PA, TCCF, EVIE	"Why Privacy Matters".	When it comes to online privacy, many who skip over the subject have said: "I have nothing to hide, so I'm okay". It's a response to which some experts in the field of privacy point out, even if you're alone in your home, would you be okay with someone watching through your window and taking notes on everything you do the entire day? Because that is essentially what's happening online right now, and it's legal.	Raise privacy awareness through control and fear.
PA, TCCF, EVIE	Protecting Personal Privacy.	(animated) This animated video explains how your exposed personal data can get you in trouble.	Raise privacy awareness, enhance knowledge of privacy concerns and privacy risk perception through control and fear.
PA, PC, EVIE	Why Care About Internet Privacy?	(animated) Whenever you browse the Internet, websites are collecting information about you and using it to fuel their businesses. They use your information to display relevant ads, to sell you products you might be interested in, and more.If you're okay with companies collecting your information, that's fine. If you're not, there are steps you can take to lessen the risk.	Increase privacy awareness and enhance knowledge of privacy concerns.
PA, PC, EVIE	Privacy Matters.	(animated). This video shows how private data exposition can hurt your job position.	Increase privacy awareness and enhance knowledge of privacy concerns.
PA, PC, EVIE	Online Privacy for Kids—Internet Safety and Security for Kids.	(animated). Social media is a great tool to communicate with our family and friends but it's important to be mindful of what we post, where we post it and who we share it with. In this educational video we're going to give you advice on how to protect our online privacy. We should be careful with what we share, even more so if it's personal information that we wouldn't like other people to know about. Sharing is a responsibility.	Increase privacy awareness and enhance knowledge of privacy concerns among kids.
PA, PC, EVIE	Online safety Staying safe online.	(animated). Learn how to stay safe and act responsibly when using the internet in school and at home.	Increase privacy awareness and enhance knowledge of privacy concerns among kids.
PA, PC, EVIE	Cyber Security for kids | Internet Safety Tips for Kids.	This video talks about the importance of password, protecting personal information, limiting screen time etc.	Increase privacy awareness and enhance knowledge of privacy concerns among kids.
PA, PC, PRP, EVIE	NetSafe Episode 11: Protect Your Personal Information.	This video explains why keeping personal information private is so important, and it offers tips on how to do it.	Increase privacy awareness and enhance knowledge of privacy concerns through showing the privacy risks.
PA, TCCF, EVIE	"Social Media Privacy: How to Be Safe" by Norton	This video provides tips for protecting your privacy on social media platforms.	Increase privacy awareness and control.
PA, EVIE	"Privacy Matters" by Mozilla	This video highlights the importance of privacy and provides tips for protecting your online privacy	Increase privacy awareness and confidence through education.
PA, PC, EVIE	"The Cost of Privacy" by Vox	This video explores the trade-offs between privacy and convenience in our digital lives.	Increase privacy awareness and enhance knowledge of privacy concerns.

Table A3. Practical assessment items.

Activated Factor(s)	Simulator Name	Short Description
PA, TCCF, EVIE	Privacy Choices	https://www.telus.com/en/wise/parents/privacy-quiz (accessed on 28 December 2023)
PA, EVIE	Privasim	Privasim is a simulator game where you play as an app company, collect users, mine data, and sell data to get rich. Avoid cyber attacks, fight legal battles and get Influencers to join your app. https://privasim.itch.io/privacysimulator (accessed on 28 December 2023)
PA, PC, EVIE	Data Detox Kit	Take control of your digital privacy, security, and well-being, learn about tackling misinformation, control your health data, find resources for youth and families, and browse our Alternative App Centre and workshop materials. Meet our partners to get a glimpse into the global movement of the Data Detox Kit. https://datadetoxkit.org/en/home (accessed on 28 December 2023)

Table A3. *Cont.*

Activated Factor(s)	Simulator Name	Short Description
PA, PC, EVIE	The Realistic Facebook Privacy Simulator	https://www.tomscott.com/usvsth3m/realistic-facebook-privacy-simulator/ (accessed on 28 December 2023)
PA, EVIE	Privacy Scores	Learn about your privacy settings and how they compare to others. It can also help you to identify areas where you can improve your privacy settings.

Table A4. Gamification items.

Game Name	Short Description
Privacy Badger	This is a browser extension game that teaches users how to protect their online privacy by blocking ads and trackers
Data Dealer	This is a web-based game that simulates the buying and selling of personal data. Players learn about data privacy issues and how to protect their information
The Glass Room	This is a physical exhibition that can be turned into a game. Visitors learn about data privacy and security by engaging with interactive exhibits
Keep Calm and Log On	This is a card game that teaches players how to protect their online privacy by recognizing different threats and taking appropriate measures
Cryptoy	This is a mobile game that teaches players about encryption and digital security by challenging them to solve puzzles

Table A5. Privacy behavior quizzes items.

Quiz Name	Short Description
Online Privacy Quiz	This quiz, created by the Electronic Frontier Foundation (EFF), tests your knowledge of online privacy issues and helps you learn how to protect your personal information online.
Privacy IQ Quiz	This quiz, created by the Privacy Rights Clearinghouse, tests your knowledge of privacy laws and practices in the United States.
Data Privacy Quiz	This quiz, created by the National Cyber Security Alliance (NCSA), tests your knowledge of data privacy and security best practices.
Facebook Privacy Quiz	This quiz, created by Facebook, helps you understand how to manage your privacy settings on the social media platform
Google Privacy Quiz	This quiz, created by Google, tests your knowledge of how Google collects and uses your data.

Appendix D. Experimental Environment Setup

- Google's accounts and tools

We constructed our experimental environment during the environment setup phase. Specifically, we created a central Gmail account (IonianUniversityLab@gmail.com) to which all other accounts will be linked. Then, we created participant accounts (ionianuniversity-labvictim1-9@gmail.com), and tested per device that we can through the embedded application by typing per account the address https://www.google.com/android/find/ (accessed on 28 December 2023) in a browser to confirm that we can pinpoint the exact location of the device and whether it is moving, the WiFi network it is connected to (SSID), and whether it is currently charging (battery level 100%). The purpose of creating these accounts is to demonstrate to the participants, via Google Timeline, that each of their movement activities can be recorded, allowing for the creation of personalized patterns, such as when they leave or return home each day and if they use WiFi or mobile data. As demonstrated in our previous research [98], all of these data can be extracted by any mobile application that is installed on our device and has access to the corresponding rights. As a reminder, the respective application's installation file (manifest apk package) is sufficient. To ensure participants' privacy and security, all data will be collected in a separate virtual machine per participant as it is pictured in Figure A6. Each virtual machine for the safety and privacy of the participants will be safely deleted upon the publication of the experiment.

Two lines of code within the manifest file, for instance, are sufficient for an application to access our website (Figure A1).

```
<manifest ... >
  <!-- Always include this permission -->
  <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />

  <!-- Include only if your app benefits from precise location access. -->
  <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
</manifest>
```

Figure A1. Android's manifest example file.

- Create VPN accounts (1-click vpn)

We used a free browsing anonymizer to create streaming platform's accounts without the risk of being detected by creating multiple accounts from the same IP address. Specifically, we installed a virtual private network add-on (extension/add-on) from the browser's official app store in the browser of our choosing. We chose 1clickVPN because it has an ideal rating (5 stars) and is compatible with more than 26,000 browsers.

- Streaming Platform Account Creation

To facilitate legal monitoring of our content, we have employed a low- to no-cost strategy. First, we generated temporary email identifiers for each topic. With VPN enabled and the Asia region selected, we conducted a search for a free trial offer for an unspecified period of time and discovered numerous 30-day trials. Asia was selected because, based on our inquiry, it appeared to offer the most affordable prices compared to the other options. After creating the profile, we were required to provide a credit or debit card for continued service use. For this reason, we placed 5 euros onto a virtual prepaid crypto card (virtual prepaid crypto card) in a foreign service of our choosing. The selection of a virtual card in a foreign service was made as an additional measure of anonymity, as this particular ser-vice states that it does not share personal information with third parties (https://www.blockchain.com/card (accessed on 28 December 2023)), despite the fact that identification was not required. Notably, while multiple accounts were established, the same prepaid cryptocurrency card sufficed for each. Finally, we opted for the most affordable platform access method. Also, there was no issue with the language selection, so we chose a profile in its Greek version to ensure there were no issues locating the content or with the supported subtitles.

- Virtual Machines Creation

To ensure maximum monitoring isolation, ensuring participants' privacy and securing their data, an equal number of virtual machines were constructed. Oracle Virtual Box was chosen to construct and utilize virtual machines because it is free and open source. Windows 10 Student Edition was selected as the operating system, which is provided for free for 30 days, with the only limitation being a subtly displayed prompt to activate it. The primary factors (except enhancing participants' privacy) for utilizing virtual machines were as follows. Each Viber for PC application can have a sim card attached, making the surveillance of Viber's internal database (SQLite) simpler and more isolated. Using VMs allows us to simultaneously monitor and execute SQL scripts on all experiment participants. The purpose of using Viber for PC and its built-in platform is explained in the following section. Each virtual machine was configured with 2 10th-generation Intel i7 cores, 4 GB RAM, and 20 GB SSD on a 32 GB RAM system. The reason for the low computing power requirements was that only the most essential software would be installed, and in order to extricate the data, a large number of VMs would need to be open in parallel, so we avoided a more expensive solution.

- Viber και SQLite.

The objective of this application is to extract as much information as possible about the participants' actual behavior. According to our previous research [98], if an advanced user and developer installs both Viber for Desktop and the SQLite Browser for direct access to the local database of his Viber account (SQLite DB), he is presented with a set

of options. First, as soon as the application synchronizes with his Google or iOS account, he can automatically view and modify a set of data through the SQLite browser. For instance, it can determine how many of its contacts have Viber installed (ViberContact = 1), if they have uploaded a photo to their profile (DownloadID = "not null"), and their last login date in unix date and time format, as well as perform various types of SQL queries. Our research at the time demonstrated that, with proper management and methodology (Figures A2 and A3), it is possible to identify a group of unknown individuals with a success rate of greater than 85 percent. The purpose of this application is to transform all collected data into relevant information. In the same study [98], we demonstrated that the methodology we developed enabled us to reveal various behavioral patterns of the research participants at the time, such as the time of morning awakening and evening sleep, arrival at work, and a different pattern of behavior during the weekends (Figures A4 and A5).

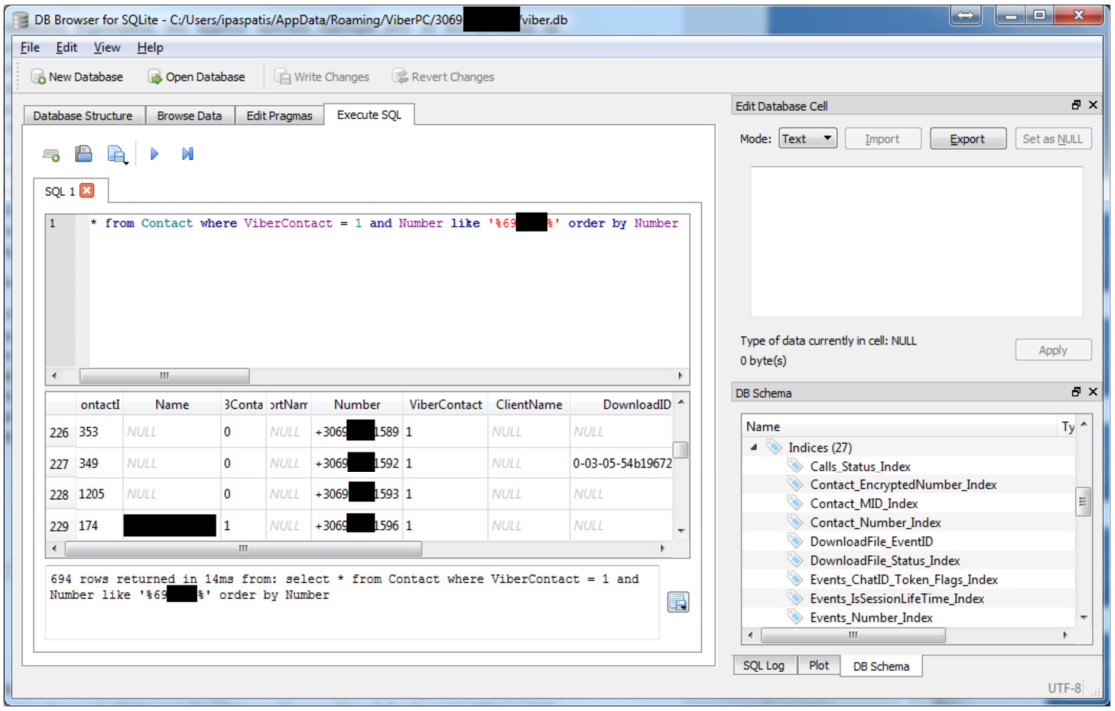

Figure A2. Viber's SQLite Database derived from [98] research.

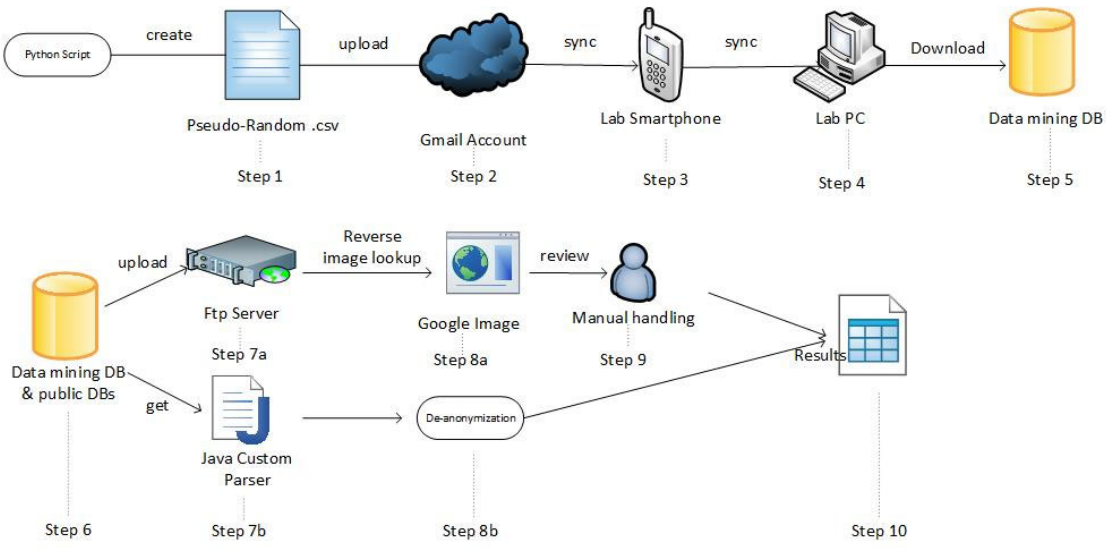

Figure A3. Paspatis et al. [98] de-anonymization methodology.

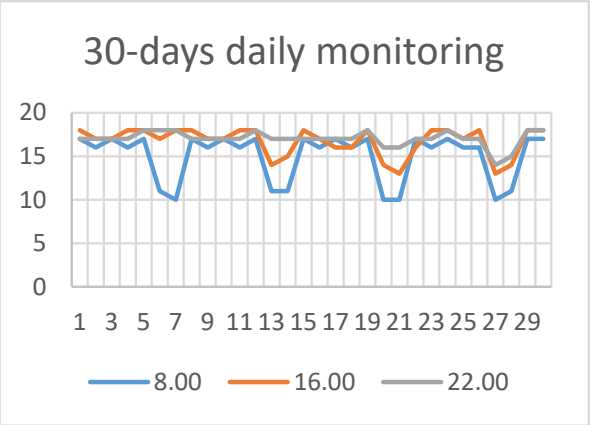

Figure A4. Daily monitoring results obtained from [98].

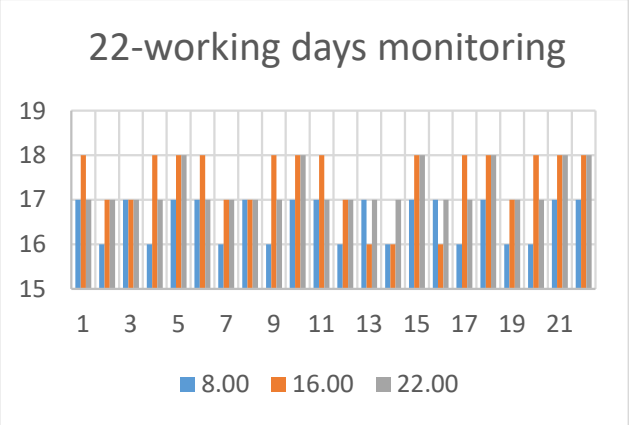

Figure A5. Working days monitoring results obtained from [98].

- Experimental Framework Tools

As we mentioned, multiple free to use software tools were selected for use throughout the experiment. Each tool is described in Table A6, while Figure A6 includes the experimental design from the virtual machines's perspective.

Table A6. Experimental environment tools.

Application/Software	Connected Software	Target
Virtual Machine	Google Account	Google Account Management
	Viber For Desktop	Viber Account Management
	Streaming Platform Account	Content Tracking Control
Google Account	Family Link	Location finding, pattern formation
	Find my phone	Location finding, pattern formation
	Timeline	Participant movement tracking
	YouTube progress	Content Monitoring Validation
Viber For Desktop	SQLite DB Browser	Finding patterns and participant information
Streaming Platform Account	Streaming Platform	Content Monitoring Validation

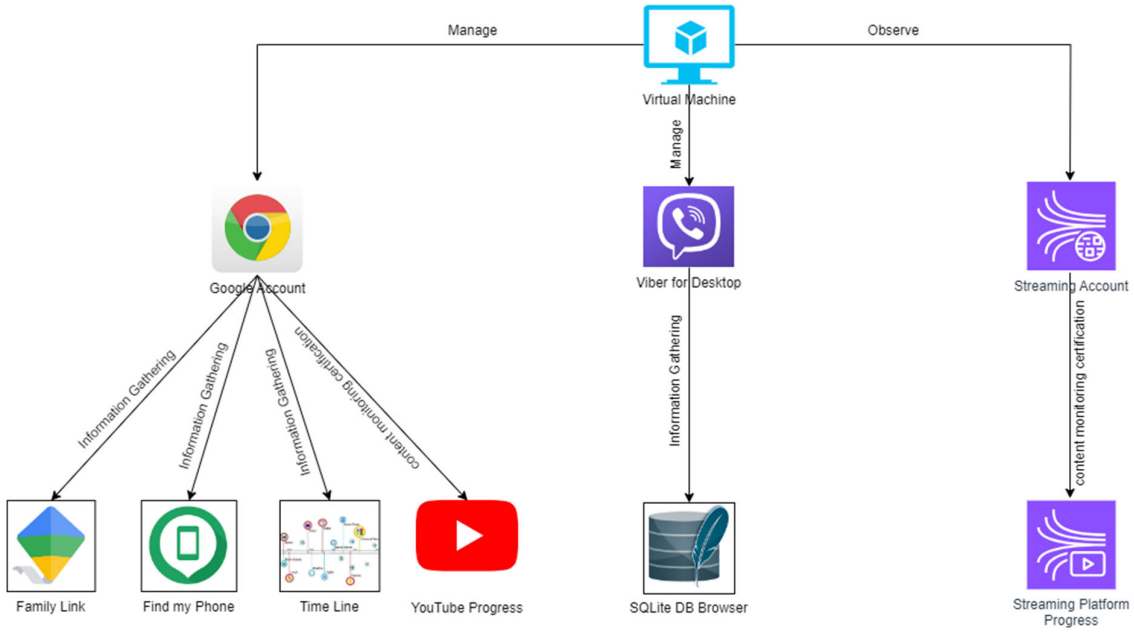

Figure A6. Environment setup representation.

- Limitations and Challenges

Throughout the preparation and execution of our experiment, we faced many obstacles and constraints arising from the chosen tools. An initial constraint we faced was the inability to monitor many SIM cards on a single virtual machine using "Viber for Desktop" and "SQLite Browser". Although employing the Windows switch account feature may resolve the current problem, it would thereafter prevent us from concurrently monitoring several databases or extracting data from their databases simultaneously using SQL queries. To address this issue, we established many instances of virtual machines and successfully resolved it. This resulted in a RAM allocation problem, as each Virtual Machine required a minimum of 4 GB of RAM, totaling 32 GB for the entire infrastructure. In order to resolve this problem, we opted to replace the selected version of Windows with a lightweight variant known as Tiny11, which required less than half the amount of RAM compared to our initial choice of operating system. Another problem we faced was the lack of support in Google Timeline for extracting a specific time period. Instead, it simply allows for downloading all of the recorded historical data. We experimented with various browser add-ons in an attempt to overcome the issue, but we could not get the anticipated outcomes. Consequently, we developed a bespoke Python script that temporarily resolved the issue, but requiring us to modify the code slightly and rerun the script whenever we needed new data. This involves basic programming proficiency, but we should strive for a long-term solution that does not necessitate the aforementioned skills. Regarding the ethical surveillance aspect, we plan to exclude it from our architecture as it evolves. Meanwhile, we intend to collect data solely using SQL queries and programming scripts. Subsequently, the obtained data can be processed using K-anonymity techniques to reduce the disclosure of personal information, street names, and specific locations even to the research team.

References

1. Thierer, A.D. *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*; Elsevier Inc.: Amsterdam, The Netherlands, 2015; Volume 21. [CrossRef]
2. Rose, K.; Eldridge, S.; Chapin, L. The internet of things: An overview. *Internet Soc.* **2015**, *80*, 1–50.
3. Menard, P.; Bott, G.J. Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Comput. Secur.* **2020**, *95*, 101856. [CrossRef]
4. Tsohou, A.; Kosta, E. Enabling valid informed consent for location tracking through privacy awareness of users: A process theory. *Comput. Law Secur. Rev.* **2017**, *33*, 434–457. [CrossRef]

5. Kokolakis, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Secur.* **2017**, *64*, 122–134. [CrossRef]
6. Hallam, C.; Zanella, G. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Comput. Hum. Behav.* **2017**, *68*, 217–227. [CrossRef]
7. Li, H.; Luo, X.R.; Zhang, J.; Xu, H. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Inf. Manag.* **2017**, *54*, 1012–1022. [CrossRef]
8. Gerber, N.; Gerber, P.; Volkamer, M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Comput. Secur.* **2018**, *77*, 226–261. [CrossRef]
9. Bless, C.; Dötlinger, L.; Kaltschmid, M.; Reiter, M.; Kurteva, A.; Roa-Valverde, A.J.; Fensel, A. Raising awareness of data sharing consent through knowledge graph visualisation. In *Further with Knowledge Graphs*; Wageningen University & Research: Wageningen, The Netherlands, 2021; Volume 53, pp. 44–57. [CrossRef]
10. Mathews-Hunt, K. CookieConsumer: Tracking online behavioural advertising in Australia. *Comput. Law Secur. Rev.* **2016**, *32*, 55–90. [CrossRef]
11. Palos-Sanchez, P.; Saura, J.R.; Martin-Velicia, F. A study of the effects of programmatic advertising on users' concerns about privacy overtime. *J. Bus. Res.* **2019**, *96*, 61–72. [CrossRef]
12. Hinds, J.; Williams, E.J.; Joinson, A.N. "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *Int. J. Hum.-Comput. Stud.* **2020**, *143*, 102498. [CrossRef]
13. Paspatis, I.; Tsohou, A.; Kokolakis, S. How Is Privacy Behavior Formulated? *A Review of Current Research and Synthesis of Information Privacy Behavioral Factors. Multimodal Technol. Interact.* **2023**, *7*, 76. [CrossRef]
14. Dinev, T.; Bellotto, M.; Hart, P.; Russo, V.; Serra, I.; Colautti, C. Privacy calculus model in e-commerce–a study of Italy and the United States. *Eur. J. Inf. Syst.* **2006**, *15*, 389–402. [CrossRef]
15. The General Data Protection Regulation (GDPR). Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 23 January 2024).
16. Lei Geral de Proteção de Dados (LGDP). Available online: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (accessed on 23 January 2024).
17. Personal Information Protection Act (PIPA). Available online: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01 (accessed on 23 January 2024).
18. Personal Data Protection Act (PDPA). Available online: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act (accessed on 23 January 2024).
19. Rogers, R.W.; Prentice-Dunn, S. Protection motivation theory. In *Handbook of Health Behavior Research 1: Personal and Social Determinants*; Hardcover; Gochman, D.S., Ed.; Plenum Press: New York, NY, USA, 1997; pp. 113–132. ISBN 0-306-45443-2.
20. Chakraborty, R.; Vishik, C.; Rao, H.R. Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decis. Support Syst.* **2013**, *55*, 948–956. [CrossRef]
21. Hofstra, B.; Corten, R.; Van Tubergen, F. Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Comput. Hum. Behav.* **2016**, *60*, 611–621. [CrossRef]
22. Jiang, J. Social Login Acceptance: A DIF Study of Differential Factors. In Proceedings of the 22nd Pacific Asia Conference on Information Systems (PACIS 2018), Yokohama, Japan, 26–30 June 2018; Volume 20, p. 20. Available online: https://aisel.aisnet.org/pacis2018/20 (accessed on 1 May 2023).
23. Park, Y.J. Do men and women differ in privacy? Gendered privacy and (in) equality in the Internet. *Comput. Hum. Behav.* **2015**, *50*, 252–258. [CrossRef]
24. Reynolds, B.; Venkatanathan, J.; Gonçalves, J.; Kostakos, V. Sharing ephemeral information in online social networks: Privacy perceptions and behaviours. In Proceedings of the Human-Computer Interaction–INTERACT 2011: 13th IFIP TC 13 International Conference, Lisbon, Portugal, 5–9 September 2011; Proceedings, Part III 13. Springer: Berlin/Heidelberg, Germany, 2011; pp. 204–215. [CrossRef]
25. Lankton, N.K.; McKnight, D.H.; Tripp, J.F. Facebook privacy management strategies: A cluster analysis of user privacy behaviors. *Comput. Hum. Behav.* **2017**, *76*, 149–163. [CrossRef]
26. Li, C.; Chau, P.Y. Leveraging communication tools to reduce consumers' privacy concern in the on-demand services: An extended SOR Model of perceived control and structural assurance. In Proceedings of the PACIS 2019 Proceedings, Xi'an, China, 8–12 July 2019; Volume 48. Available online: https://aisel.aisnet.org/pacis2019/48 (accessed on 5 April 2023).
27. Dhir, A.; Kaur, P.; Lonka, K.; Nieminen, M. Why do adolescents untag photos on Facebook? *Comput. Hum. Behav.* **2016**, *55*, 1106–1115. [CrossRef]
28. Yu, L.; Li, H.; He, W.; Wang, F.K.; Jiao, S. A meta-analysis to explore privacy cognition and information disclosure of internet users. *Int. J. Inf. Manag.* **2020**, *51*, 102015. [CrossRef]
29. Shane-Simpson, C.; Manago, A.; Gaggi, N.; Gillespie-Lynch, K. Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Comput. Hum. Behav.* **2018**, *86*, 276–288. [CrossRef]
30. Ioannou, A.; Tussyadiah, I.; Lu, Y. Privacy concerns and disclosure of biometric and behavioral data for travel. *Int. J. Inf. Manag.* **2020**, *54*, 102122. [CrossRef]

31. Wilson, D.W.; Schuetzler, R.M.; Dorn, B.; Proudfoot, J.G. *When Disclosure Is Involuntary: Empowering Users with Control to Reduce Concerns*; Criss Library: Omaha, NE, USA, 2015; Volume 17. Available online: https://digitalcommons.unomaha.edu/isqafacproc/17 (accessed on 1 May 2023).
32. Ioannou, A.; Tussyadiah, I. Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technol. Soc.* **2021**, *67*, 101774. [CrossRef] [PubMed]
33. Nikkhah, H.R.; Sabherwal, R. Mobile cloud-computing applications: A privacy cost-benefit model. In Proceedings of the Americas Conference on Information Systems, Boston, MA, USA, 10–12 August 2017. Available online: https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/11 (accessed on 24 January 2024).
34. Van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480. [CrossRef]
35. Jordaan, Y.; Van Heerden, G. Online privacy-related predictors of Facebook usage intensity. *Comput. Hum. Behav.* **2017**, *70*, 90–96. [CrossRef]
36. Fox, G.; Tonge, C.; Lynn, T.; Mooney, J. Communicating compliance: Developing a GDPR privacy label. In Proceedings of the AMCIS 2018 Proceedings, New Orleans, LA, USA, 16–18 August 2018; Volume 30. Available online: https://aisel.aisnet.org/amcis2018/Security/Presentations/30 (accessed on 24 January 2024).
37. Risius, M.; Baumann, A.; Krasnova, H. Developing a new paradigm: Introducing the intention-behaviour gap to the privacy paradox phenomenon. In Proceedings of the Twenty-Eigth European Conference on Information Systems (ECIS2020), Marrakesh, Morocco, 15–17 June 2020. Available online: https://aisel.aisnet.org/ecis2020_rp/150 (accessed on 24 January 2024).
38. Jozani, M.; Ayaburi, E.; Ko, M.; Choo, K.K.R. Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Comput. Hum. Behav.* **2020**, *107*, 106260. [CrossRef]
39. Sharma, S.; Crossler, R.E. Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electron. Commer. Res. Appl.* **2014**, *13*, 305–319. [CrossRef]
40. Zhang, Y.; He, W.; Peng, L. How perceived pressure affects users' social media fatigue behavior: A case on WeChat. *J. Comput. Inf. Syst.* **2022**, *62*, 337–348. [CrossRef]
41. Mager, S.; Kranz, J. Consent Notices and the Willingness-to-Sell Observational Data: Evidence from User Reactions in the Field. In Proceedings of the ECIS 2021, 14–16 June 2021; Research Papers. Volume 89. Available online: https://aisel.aisnet.org/ecis2021_rp/89 (accessed on 24 January 2024).
42. Hew, J.J.; Tan, G.W.H.; Lin, B.; Ooi, K.B. Generating travel-related contents through mobile social tourism: Does privacy paradox persist? *Telemat. Inform.* **2017**, *34*, 914–935. [CrossRef]
43. Xu, H.; Parks, R.; Chu, C.H.; Zhang, X.L. Information disclosure and online social networks: From the case of Facebook news feed controversy to a theoretical understanding. In Proceedings of the 16th Americas Conference on Information Systems 2010 (AMCIS 2010), Lima, Peru, 12–15 August 2010; Volume 7, p. 503. Available online: https://aisel.aisnet.org/amcis2010/503 (accessed on 24 January 2024).
44. Gómez-Barroso, J.L. Experiments on personal information disclosure: Past and future avenues. *Telemat. Inform.* **2018**, *35*, 1473–1490. [CrossRef]
45. Schomakers, E.M.; Lidynia, C.; Müllmann, D.; Ziefle, M. Internet users' perceptions of information sensitivity–insights from Germany. *Int. J. Inf. Manag.* **2019**, *46*, 142–150. [CrossRef]
46. Choi, H.; Park, J.; Jung, Y. The role of privacy fatigue in online privacy behavior. *Comput. Hum. Behav.* **2018**, *81*, 42–51. [CrossRef]
47. European Union. EU Digital COVID Certificate. Available online: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en (accessed on 24 April 2023).
48. Kraus, L.; Wechsung, I.; Möller, S. Psychological needs as motivators for security and privacy actions on smartphones. *J. Inf. Secur. Appl.* **2017**, *34*, 34–45. [CrossRef]
49. Schreiber, T.; Deuker, A.; Albers, A.; Neves, M. The Privacy Trade-Off: App Usage on OSN. In Proceedings of the AMCIS 2013, Chicago, IL, USA, 15–17 August 2013.
50. Chou, H.L.; Liu, Y.L.; Chou, C. Privacy behavior profiles of underage Facebook users. *Comput. Educ.* **2019**, *128*, 473–485. [CrossRef]
51. Keith, M.; Ngo, N.; Babb, J. The effects of consumer self-regulation on information disclosure over mobile devices. In Proceedings of the International Conference on Interaction Sciences, AMCIS 2014 Proceedings, Savannah, GA, USA, 7–9 August 2014; Volume 8. Available online: https://aisel.aisnet.org/amcis2014/MobileComputing/GeneralPresentations/8 (accessed on 24 April 2023).
52. Renaud, K.; Zimmermann, V. Ethical guidelines for nudging in information security & privacy. *Int. J. Hum.-Comput. Stud.* **2018**, *120*, 22–35.
53. Paspatis, I.; Tsohou, A.; Kokolakis, S. AppAware: A policy visualization model for mobile applications. *Inf. Comput. Secur.* **2020**, *28*, 116–132. [CrossRef]
54. Paspatis, I.; Tsohou, A. How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors. *J. Cybersecur. Priv.* **2023**, *3*, 396–415. [CrossRef]
55. Kolb, D.A. *Experiential Learning: Experience as the Source of Learning and Development*; FT Press: Upper Saddle River, NJ, USA, 2014; ISBN 0132952610.
56. Jarvis, P. *Adult Education and Lifelong Learning: Theory and Practice*, 3rd ed.; Routledge: Abingdon, UK, 2004. [CrossRef]
57. Dewey, J. *Experience and Education*; Macmillan: New York, NY, USA, 1938. [CrossRef]

58. Freire, P. *Teachers as Cultural Workers—Letters to Those Who Dare to Teach*; Westview Press: Boulder, CO, USA, 1998; p. 100, ISBN 978-0-8133-4329-7.
59. Rogers, A. *Adult Education*; Metaichmio Publications: Athens, Greece, 1999; Volume 1, ISBN 978-960-566-840-2.
60. Kokko, A. *Adult Education Methodology: Theoretical Framework and Learning Conditions*; Patras EAP: Patras, Greece, 2005; Volume A.
61. Mezirow, J. *Transformative Dimensions of Adult Learning*; Jossey-Bass: San Fransisco, CA, USA, 1991; ISBN -1-55542-339-6.
62. Mezirow, J. Transformative learning and social action: A response to Inglis. *Adult Educ. Q.* **1998**, *49*, 70–72. [CrossRef]
63. Mezirow, J. On Critical Reflection: A Review of Mezirow's Theory and Its Operationalization. *Hum. Resour. Dev. Rev.* **2016**, *15*, 3–28. [CrossRef]
64. Mezirow, J. *Transformative Learning*; Metaichmio Publications: Athens, Greece, 2006; Volume 1, ISBN 978-960-455-226-9.
65. Taylor, W.E. The Theory and Practice of Transformative Learning: A Critical Review. In *ERIC Clearinghouse on Adult, Career, and Vocational Education*; The Ohio State University: Columbus, OH, USA, 1998. Available online: https://eric.ed.gov/?id=ED423422 (accessed on 31 January 2024).
66. Boud, D.; Keohg, R.; Walker, D. *Reflection: Turning Experience into Learning*; Kogan Press: New York, NY, USA, 2002; ISBN 9781315059051.
67. Tass, P.A. A model of desynchronizing deep brain stimulation with a demand-controlled coordinated reset of neural subpopulations. *Biol. Cybern.* **2003**, *89*, 81–88. [CrossRef]
68. Pavlov, I.P. Conditioned Responses. In *Readings in General Psychology*; Dennis, W., Ed.; Prentice-Hall, Inc.: Upper Saddle River, NJ, USA, 1949; pp. 249–267. [CrossRef]
69. Bandura, A. Social Learning through Imitation. In *Nebraska Symposium on Motivation*; Jones, M.R., Ed.; University of Nebraska Press: Lincoln, NE, USA, 2018; Volume 9, pp. 211–269.
70. Ainsworth, M.D.S.; Blehar, M.C.; Waters, E.; Wall, S. *Patterns of Attachment: A Psychological Study of the Strange Situation*; Erlbaum: Hillsdale, NJ, USA, 1978. Available online: https://psycnet.apa.org/record/1980-50809-000 (accessed on 8 September 2023).
71. Watson, J.B.; Rayner, R. Conditioned emotional reactions. *J. Exp. Psychol.* **1920**, *3*, 1–14. Available online: https://psycnet.apa.org/record/2006-01667-001 (accessed on 8 September 2023).
72. Asch, S.E. Effects of group pressure upon the modification and distortion of judgments. In *Groups, Leadership, and Men*; Guetzkow, H., Ed.; Carnegie Press: Lancaster, UK, 1951; pp. 177–190. Available online: https://psycnet.apa.org/record/1952-00803-001 (accessed on 8 September 2023).
73. Becker, H.S. *Outsiders: Studies in the Sociology of Deviance*; Free Press: Glencoe, IL, USA, 1963. Available online: https://psycnet.apa.org/record/1965-08393-000 (accessed on 8 September 2023).
74. Gipps, C. *Beyond Testing (Classic Edition): Towards a Theory of Educational Assessment*; Routledge: Abingdon, UK, 2011. [CrossRef]
75. Leenen, L.; van Vuuren, J.J. Framework for the cultivation of a military cybersecurity culture. In Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019), Stellenbosch, South Africa, 28 February–1 March 2019; pp. 212–220. Available online: http://www.cair.org.za/sites/default/files/2020-02/ (accessed on 8 September 2023).
76. Oh, B.M.; Byun, H.; Krishnamoorthy, A. Privacy Issues on Social Media: A Tool for Raising Privacy Awareness on Social Media. Available online: https://www.proquest.com/openview/6081551115e65038b1797e1f71897f6f/1?pq-origsite=gscholar&cbl=396500 (accessed on 8 September 2023).
77. Deterding, S.; Sicart, M.; Nacke, L.; O'Hara, K.; Dixon, D. Gamification: Using game-design elements in non-gaming contexts. In Proceedings of the CHI'11 Extended Abstracts on Human Factors in Computing Systems, Vancouver, BC, Canada, 7–12 May 2011; pp. 2425–2428. [CrossRef]
78. Mavroeidi, A.G.; Kitsiou, A.; Kalloniatis, C. The role of gamification in privacy protection and user engagement. In *Security and Privacy From a Legal, Ethical, and Technical Perspective*; IntechOpen Limited: London, UK, 2020; Volume 79. [CrossRef]
79. Karagiannis, S.; Papaioannou, T.; Magkos, E.; Tsohou, A. Game-based information security/privacy education and awareness: Theory and practice. In *European, Mediterranean, and Middle Eastern Conference on Information Systems*; Springer International Publishing: Cham, Switzerland, 2020; pp. 509–525. [CrossRef]
80. Drozd, O.; Kirrane, S. Privacy CURE: Consent comprehension made easy. In Proceedings of the ICT Systems Security and Privacy Protection: 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, 21–23 September 2020; Proceedings 35. Springer International Publishing: Cham, Switzerland, 2020; pp. 124–139. [CrossRef]
81. Sofia-Niovi, M.; Christos, K. Virtual Reality as a mean for increasing privacy awareness: The escape room example. In Proceedings of the 26th Pan-Hellenic Conference on Informatics (PCI 2022), Athens, Greece, 25–27 November 2022; ACM: New York, NY, USA, 2022. 9p. [CrossRef]
82. Mavroeidi, A.G.; Kitsiou, A.; Kalloniatis, C.; Gritzalis, S. Gamification vs. privacy: Identifying and analysing the major concerns. *Future Int.* **2019**, *11*, 67. [CrossRef]
83. Mavroeidi, A.G.; Kitsiou, A.; Kalloniatis, C. *Gamification: A Necessary Element for Designing Privacy Training Programs*; IntechOpen Limited: London, UK, 2021. [CrossRef]
84. Henne, B.; Szongott, C.; Smith, M. Towards a mobile security & privacy simulator. In Proceedings of the 2011 IEEE Conference on Open Systems, Langkawi, Malaysia, 25–28 September 2011; pp. 95–100. Available online: https://ieeexplore.ieee.org/abstract/document/6079294 (accessed on 8 September 2023).
85. Miller, W.R.; Rollnick, S. *Motivational Interviewing: Helping People Change*; Hardcover; Guilford Press: New York, NY, USA, 2012; ISBN 978-1-60918-227-4.

86. Naar, S.; Safren, S.A. *Motivational Interviewing and CBT: Combining Strategies for Maximum Effectiveness*; Guilford Press: New York City, NY, USA, 2017. Available online: https://psycnet.apa.org/record/2017-26282-000 (accessed on 8 September 2023).
87. Towne, K.; Campagna, M.; Spohn, R.; Richey, A. "Put it in your toolbox": How vocational programs support formerly incarcerated persons through reentry. *Crime Delinq.* 2023, 69, pp. 316–341. Available online: https://journals.sagepub.com/doi/full/10.1177/00111287221098581 (accessed on 8 September 2023).
88. Cun, L.; Hu, L.; Hu, K.; Huang, H.; Deng, N.; Wen, J.; Yang, L.; Zhao, Y. Effect of Cognitive-behavioral Change Model-based Online Health Education in Hypertension Management. *Chin. Gen. Pract.* **2022**, *25*, 1984. [CrossRef]
89. Dali, K.; Hohmann, G. Preserving the Wonder of Stories: The Role of Reflection in Reading Education in Library and Information Science Programs. *J. Educ. Libr. Inf. Sci.* **2023**, *64*, 206–229. [CrossRef]
90. Dols, J.M.F.; Russell, J.A. (Eds.) Natural facial expression: A view from psychological constructionism and pragmatics. In *The Science of Facial Expression*; Oxford University Press: Oxford, UK, 2017; pp. 457–475. ISBN 978-0-19-061350-1.
91. De Berardis, D.; Fornaro, M.; Orsolini, L. "No Words for Feelings, Yet!" Exploring Alexithymia, Disorder of Affect Regulation, and the "Mind-Body" Connection. *Front. Psychiatry* **2020**, *11*, 593462. [CrossRef] [PubMed]
92. Rufer, M.; Hand, I.; Braatz, A.; Alsleben, H.; Fricke, S.; Peter, H. A prospective study of alexithymia in obsessive-compulsive patients treated with multimodal cognitive-behavioral therapy. *Psychother. Psychosom.* **2004**, *73*, 101–106. [CrossRef] [PubMed]
93. COPE Core Practices. Available online: https://publicationethics.org/core-practices (accessed on 23 January 2024).
94. Holmes, C.C.; Adams, N.M. Likelihood Inference in Nearest-Neighbour Classification Models. *Biometrika* **2003**, *90*, 99–112. [CrossRef]
95. Murdoch, M.; Simon, A.B.; Polusny, M.A.; Bangerter, A.K.; Grill, J.P.; Noorbaloochi, S.; Partin, M.R. Impact of different privacy conditions and incentives on survey response rate, participant representativeness, and disclosure of sensitive information: A randomized controlled trial. *BMC Med. Res. Methodol.* **2014**, *14*, 90. [CrossRef]
96. Fisher, R.A. Statistical methods for research workers. In *Breakthroughs in Statistics: Methodology and Distribution*; Springer: New York, NY, USA, 1970; pp. 66–70. [CrossRef]
97. Cronbach, L.J. Coefficient alpha and the internal structure of tests. *Psychometrika* **1951**, *16*, 297–334. [CrossRef]
98. Paspatis, I.; Tsohou, A.; Kokolakis, S. Mobile application privacy risks: Viber users' de-anonymization using public data. In Proceedings of the MCIS 2017, Genoa, Italy, 4–5 September 2017; Proceedings 32. Available online: https://aisel.aisnet.org/mcis2017/32 (accessed on 24 January 2024).