Arzoglou, Ektor; Kortesniemi, Yki; Ruutu, Sampsa; Elo, Tommi

The Role of Privacy Obstacles in Privacy Paradox: A System Dynamics Analysis

Published in:
Systems

DOI:
10.3390/systems11040205

Published: 19/04/2023

Document Version
Publisher's PDF, also known as Version of record

systems

MDPI

Article

The Role of Privacy Obstacles in Privacy Paradox: A System Dynamics Analysis

Ektor Arzoglou *, Yki Kortesniemi, Sampsa Ruutu and Tommi Elo

Department of Information and Communications Engineering, School of Electrical Engineering, Aalto University, PL 15600, 00076 Aalto, Finland

* Correspondence: ektor.arzoglou@aalto.fi

Abstract: People use social media to achieve particular gratifications despite expressing concerns about the related privacy risks that may lead to negative consequences. This inconsistency between privacy concerns and actual behaviour has been referred to as the privacy paradox. Although several possible explanations for this phenomenon have been provided over the years, they each consider only some of the obstacles that stand in the way of informed and rational privacy decisions, and they usually assume a static situation, thus neglecting the changes taking place over time. To overcome these limitations, this article incorporates all the key privacy obstacles into a qualitative system dynamics model and examines the conditions under which the privacy paradox emerges over time in the context of social media. The results show that the privacy obstacles prevent adequately accounting for the negative consequences by (1) reinforcing gratifications, thus inducing social media adoption and use, while (2) hampering the realisation of (all) negative consequences, thus reducing the motivation for social media discard. Moreover, gratifications kick off early and often seem to dominate even major long-term negative consequences, thereby resulting in users becoming only gradually concerned about privacy, by which time they are usually deeply engaged in the platform to consider discarding, and therefore arriving in a paradoxical situation that seems not viable to escape from (i.e., the boiling frog syndrome). Conversely, major short-term negative consequences are more likely to conflict with gratifications already earlier, thereby resulting in users becoming less engaged, more concerned, and therefore still able to discard the platform, thus resolving the paradoxical situation.

Keywords: digital platforms; privacy; privacy obstacles; privacy paradox; social media; system dynamics

Citation: Arzoglou, E.; Kortesniemi, Y.; Ruutu, S.; Elo, T. The Role of Privacy Obstacles in Privacy Paradox: A System Dynamics Analysis. *Systems* **2023**, *11*, 205. https://doi.org/10.3390/systems11040205

Received: 17 February 2023
Revised: 27 March 2023
Accepted: 12 April 2023
Published: 19 April 2023

1. Introduction

Social media, such as Facebook and Instagram, are platforms that have changed how people interact and share experiences by acting as *mediators* between users and content [1]. Users satisfy different needs by actively constructing their online identities, to which they often attach intricate details about their private life, both for personal self-expression and professional self-promotion [2]. As a result, users draw the attention of other users with whom they engage in data sharing, hence achieving high *gratifications* and inducing further social media adoption and use.

Platforms are social infrastructures of the digital age that promote social inclusion, by offering the ability to form meaningful communities, while also presenting new privacy challenges, since they typically collect and process large amounts of personal data as a constitutive characteristic of their business models. That is, meaningful participation in society now often comes in exchange for personal data, and therefore with loss of privacy, as some kind of entrance fee [3,4]. This new social reality was one of the main motivations for the General Data Protection Regulation (GDPR), which came into effect within the European Union (EU) in 2018 to give users the right to know about and object

to the upcoming collection, processing, and dissemination of their data (Articles 12–15, 21), the right to rectify and erase their data (Articles 16–17), and the right not to be subject to automated decision-making (Article 22) [5]. However, users seem to have a limited understanding of their rights, doubt the effectiveness of their rights [6], and eventually accept that 'paying with their data' for 'free' platforms is a situation that must be learned to live with [5].

At the same time, surveys show that users express high concerns about the privacy of their data: 67% of EU citizens are concerned about not having complete control over the information they provide online, 55% are concerned about their data being collected, and 74% of US citizens are more alarmed than ever about privacy [7,8]. However, these concerns are only partially reflected in the actual behaviour of users: 43% of EU citizens provide personal information online because they are required to do so, and 69% of US citizens accept certain online privacy risks due to convenience [7,8]. This inconsistency between privacy concerns and actual behaviour has been referred to as the *privacy paradox* [9,10], which reflects this new social reality, where the benefits of social inclusion come inevitably at the cost of privacy.

Over the last couple of decades, privacy researchers have provided several possible explanations for the privacy paradox, focusing mainly on people's (in)ability to evaluate the potential benefits and costs of privacy decisions, which are affected by heuristics, cognitive biases, and social factors [11–13]. In addition, privacy researchers have identified numerous challenges, which have been condensed into eight concrete privacy obstacles [14] (see Section 3.3), that prevent the full appraisal of a situation, causing people to not be fully aware of their data being collected, analysed, and processed [3], thus diminishing the possibilities of people making informed and rational privacy decisions. However, current privacy paradox explanations consider only subsets of the eight privacy obstacles in separation, hence the pieces of the puzzle remain scattered, and the "whole picture" is still missing from current privacy literature [12].

Methodologically, previous privacy paradox studies have used mainly two cross-sectional approaches: (1) surveys, which rely on self-reported behaviour that often differs from actual behaviour, and (2) experiments, which often fail to recreate a realistic context [12]. However, actual behaviour unfolds in a dynamic manner (i.e., over time) and therefore cannot be fully explained by cross-sectional approaches.

To overcome these limitations, this article incorporates existing privacy knowledge, including all eight privacy obstacles, into a qualitative *system dynamics model* [15] and examines the conditions under which the privacy paradox emerges over time in the context of social media.

The research questions guiding this article are: *RQ1: How do the privacy obstacles affect people's privacy behaviour over time?*, and *RQ2: How do the privacy obstacles help understand the privacy paradox?* The results show that the eight privacy obstacles prevent adequately accounting for the negative consequences of adopting and using social media by (1) reinforcing gratifications, thus inducing social media adoption and use, while (2) hampering the realisation of (all) negative consequences, thus reducing the motivation for social media discard. Moreover, gratifications kick off early and often seem to dominate even major long-term negative consequences, thereby resulting in users becoming only gradually concerned about privacy, by which time they are usually deeply engaged in the platform to consider discarding, and therefore arriving in a paradoxical situation that seems not viable to escape from (i.e., the boiling frog syndrome [16]). Conversely, major short-term negative consequences are more likely to conflict with gratifications already earlier, thereby resulting in users becoming less engaged, more concerned, and therefore still able to discard the platform, thus resolving the paradoxical situation. Finally, the contributions of this article also include demonstrating the potential of system dynamics as a tool for analysing privacy behaviour.

The rest of the article is organised as follows. Section 2 summarises the social media uses and gratifications, and Section 3 reviews literature on informational privacy, privacy

paradox, and privacy obstacles. Section 4 describes the system dynamics modelling methodology, and Section 5 presents the model of the social media platform affected by the eight privacy obstacles. Section 6 analyses the model, and Section 7 discusses the prospect of addressing the privacy obstacles and therefore reducing the extent of the privacy paradox. Finally, Section 8 concludes the article.

2. Social Media Uses and Gratifications

One of the most commonly utilised frameworks for studying people's motivations to use different types of media, including social media, is the *uses and gratifications theory*, which assumes that media consumption is driven by the needs of individuals that they seek to satisfy [17]. As such, people actively search for and distinguish between different types of media and content, which is intended for specific uses in order to satisfy different cognitive, affective, and social needs and to achieve particular gratifications [18,19]. McQuail identifies four motivations for traditional media use: (1) entertainment, (2) integration and social interaction, (3) personal identity, and (4) information [20]. Although these four motivations have been found relevant and applicable to social media too, Muntinga, Moorman, and Smit extend McQuail's set by proposing two additional motivations, which are uniquely related to social media use: (5) remuneration and (6) empowerment [21].

First, the *entertainment* motivation covers gratifications related to escaping from problems and routine, relaxing, killing time, getting cultural and aesthetic enjoyment, and seeking emotional release and sexual arousal [22–26]. The second motivation is *integration and social interaction*, which covers gratifications related to the sense of belonging, the need to connect with peers and family, and the need to seek emotional support [23–28]. Third, the *personal identity* motivation covers gratifications related to constructing an identity by communicating and projecting a desired identity in order to gain self-fulfilment [24,28,29]. The fourth motivation is *information*, which covers gratifications related to seeking and sharing information, keeping up with or gaining knowledge about others and the world, and storing personal information as a means of backup [22,29,30]. Fifth, the *remuneration* motivation covers gratifications related to the expectancy to receive rewards, such as vouchers, financial discounts, promotional deals, and free samples [31,32]. Finally, the sixth motivation is *empowerment*, which covers gratifications related to voicing out discontent, fighting unfairness, providing solutions, judging inaccuracy, and encountering arguments to different views [31,33–36].

The six social media uses and gratifications are summarised in Table 1.

Table 1. Social media uses and gratifications. Adapted with permission from ref. [17]. 2020 SAGE Publications.

Motivation	Description
Entertainment	The relaxation, enjoyment, and emotional relief generated by temporarily escaping from daily routines.
Integration and social interaction	The sense of belonging (e.g., connectedness), the supportive peer groups (e.g., bandwagon), and the enhanced interpersonal connections associated with media use (e.g., community building).
Personal identity	The need to shape an identity through self-expression by sharing an image of this identity through self-presentation in order to gain self-assurance and self-recognition.
Information	The need to seek and share information, watch what others are doing (i.e., surveillance), and document personal information (i.e., lifelogging).
Remuneration	The expectancy to gain future benefits and rewards that basically stand apart from the behaviour.
Empowerment	The aim to exert influence or power on others by voicing opinions in order to enforce excellence and accuracy.

At the same time, people express concerns about the privacy risks and potential negative consequences related to social media [37]. However, previous privacy studies show that motivations to use social media do not necessarily conflict with privacy concerns, and therefore the gratifications achieved from using social media result in neither negligible nor strict privacy preferences and concerns. Hence, motivations to use social media seem to be independent from rather than aligned with the need for privacy, and for this reason people will use social media regardless of being concerned about privacy or not [38].

3. Privacy

The privacy concept has three aspects: (1) *territorial privacy*, which refers to the protection of a person's physical surroundings, (2) *privacy of the person*, referring to the protection of a person against undue interference, and (3) *informational privacy*, which refers to the control of the collection, storing, processing, and dissemination of personal data [12,39,40]. The focus of this article is restricted to the third aspect.

3.1. Informational Privacy

Two of the most influential privacy theories are those developed by Alan Westin [41] and Irwin Altman [42]. Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. [Moreover] . . . privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means" [41]. Altman defines privacy simply as "the selective control of access to the self" [42].

Both privacy theories by Westin and Altman discuss privacy as a *dynamic* process (i.e., over time) of interpersonal boundary control or regulation that can be either successful or unsuccessful. For example, in his *privacy regulation theory*, Altman differentiates between *actual* and *desired* privacy levels [42,43]. In this regard, privacy regulation is either successful, in case of an optimal privacy level (actual = desired level), or unsuccessful, in case of too much (actual $>$ desired level) (e.g., crowding) or too little (actual $<$ desired level) (e.g., social isolation) privacy. Petronio extends privacy regulation theory to develop her *communication privacy management theory* (CPM) by articulating "[a] most complicated set of dynamics" [44]. In CPM theory, individuals form their subjective privacy boundaries, which can be either completely open or completely closed. Open boundaries reflect a willingness to disclose private information while closed boundaries a tendency to conceal and protect it. These boundaries are regulated by three rules: (1) *linkage*, determining who else can know, (2) *permeability*, determining how much others can know, and (3) *ownership*, determining the rights of others over what they know. These rules essentially reflect the *control* of individuals over their private information, and they are also dynamic as they might change over time. Failure of individuals to effectively control their private information signifies a *boundary turbulence*.

However, not all people share the same privacy preferences. Westin's privacy segmentation divides the public into three (empirically- and not theoretically-derived) groups: (1) *privacy fundamentalists*, who see privacy as paramount, (2) *privacy unconcerned*, who see no need for privacy, and (3) *privacy pragmatists*, who weigh potential personal or societal benefits of information disclosure, assess privacy risks, and then decide whether they will agree or disagree with specific information activities [45,46].

While Altman's theory has a broader social interaction scope, Petronio's extension focuses on informational privacy and so does Westin's theory. Since the focus of this article is exclusively on informational privacy as well, Petronio's CPM theory acts as a key driver for the model development.

3.2. Privacy Paradox

The term 'privacy paradox' emerged from studying privacy in the context of consumer behaviour. In 2001, Brown "uncovered something of a privacy paradox" through a series of interviews with online shoppers; despite expressing high privacy concerns, consumers

were still willing to give their personal details to online retailers as long as they had something to gain in return [9,12]. Some of the most important explanations for the privacy paradox are based on: (1) privacy calculus, (2) incomplete information, bounded rationality, and decision biases, and (3) social influence [12,13,46]. The first two explanations are centred around a cost-benefit analysis in privacy decision-making that ultimately favours benefits over costs. Explanations based on privacy calculus assume a *rational assessment of privacy risks* within the cost-benefit analysis, whereas explanations based on incomplete information, bounded rationality, and decision biases assume an *irrational assessment of privacy risks*. Finally, explanations based on social influence assume that benefits are prevalent in privacy decision-making. As a result, *negligible or no assessment of privacy risks* takes place, and a thorough cost-benefit analysis cannot be performed [11].

3.2.1. Privacy Calculus

The *privacy calculus theory* studies the privacy concept from an economic point of view and assumes that privacy decisions are driven by the efforts of people to maximise their benefits [47]. For example, when making data sharing decisions, people evaluate the potential benefits of disclosure against the expected privacy costs and decide to share their data only when potential benefits outweigh expected costs [12,48]. The benefits of data sharing can be intangible, such as inner satisfaction of belonging to a community, or tangible, such as financial discounts. On the other hand, the costs of data sharing are mainly intangible and include the privacy risks and potential negative consequences of disclosure, such as data misuse by third parties or social criticism and humiliation [13]. Nevertheless, even if people decide to share their data, considering that potential benefits outweigh expected costs, they might still express concerns about their data being lost, leading to the apparent inconsistency between expressed privacy concerns (or attitude) and actual behaviour [13].

3.2.2. Incomplete Information, Bounded Rationality, and Decision Biases

The privacy calculus theory assumes that people are rational agents, who engage in high-effort cognitive processing when making privacy decisions, and it therefore neglects different *heuristics and cognitive biases* [49] that have been found to affect privacy decision-making [50,51]. For example, assuming people to have perfect foresight of all potential benefits and costs when making data sharing decisions seems practically impossible. On the contrary, people are often unaware of their data being collected [52]. As a result, their privacy decisions are based on *incomplete information*, which can lead to under- or overestimation of potential benefits and costs when making these privacy decisions. Moreover, even if people have access to complete information, they might still not be able to assess it properly because of limitations in the human cognitive processing ability. This effect has been defined as *bounded rationality* [53]. To compensate for their bounded rationality, people use different heuristics —rules of thumb— to make decisions. However, heuristics often result in imperfect decisions that suffer from cognitive biases (i.e., the resulting gaps between normative behaviour and heuristically determined behaviour) [49]. Hence, the original intention or expressed attitude towards the behaviour might not be reflected in the actual behaviour [13]. Some common examples of cognitive biases are the following:

- The *affect bias*: People tend to judge and make decisions quickly based on their current emotions, thereby underestimating the risks of things they like and overestimating the risks of things they dislike [54].
- The *availability bias*: People tend to overestimate and rely on information they can easily recall, because it might be present in the media, rather than information that is relevant [55].
- The *confirmation bias*: People tend to search for, interpret, favour, and recall information in a way that confirms or supports their beliefs or values [56].

- The *hyperbolic discounting/immediate gratification bias*: People tend to forego more rewarding future benefits in order to obtain less rewarding immediate benefits [57].
- The *optimism bias*: People tend to overestimate the likelihood of experiencing positive events and underestimate the likelihood of experiencing negative events compared to others [58].
- The *overconfidence bias*: People tend to overestimate their skills and talent [59] and often their ability to control events [60].

Finally, the imperfect decisions driven by heuristics have been argued to derive from *misperceptions of feedback* [61,62]. People fail to adequately account for the delay between their decisions and the effects of these decisions. As such, people will try to correct the unintended consequences of their decisions only when they start to realise them. Nevertheless, efforts to address previously unintended consequences might still result in further unexpected outcomes.

A privacy paradox explanation based on misperceptions of feedback is missing from current privacy literature and can be provided by the model of this article.

3.2.3. Social Influence

As social media are considered an integral part of modern life [3], non-participation for people who wish to maintain their social lives may simply be infeasible regardless of privacy preferences and concerns [63]. As a result, most people are not autonomous in their decisions to accept or reject the use of social media, since they are significantly influenced by the opinion and behaviour of their social environment [13]. In addition, while peers and family can create *social pressure* towards certain decisions, they can also create a *social stigma* for anyone who deviates from these decisions [64]. Hence, the expressed attitude is apparently echoing the unbiased opinion, but it is not necessarily reflected in the actual behaviour, which is often affected by social factors [13].

3.2.4. Privacy Paradox in Social Media

The privacy paradox remains a controversial phenomenon, with privacy researchers providing contradictory results that either support or challenge the existence of the inconsistency between privacy concerns and actual behaviour. On one hand, studies show that concerns about data misuse by service providers or third parties may cause people to configure their privacy settings [38] and even limit information disclosure [65,66]. In this case, the existence of the privacy paradox could be challenged, since privacy concerns are found to be consistent with actual behaviour. On the other hand, studies also show that certain biases, such as the tendency to connect with others who share the same characteristics and interests (i.e., similarity bias), and social factors, such as the tendency to share data in response to previous rewards (i.e., norm of reciprocity), may leverage privacy concerns and increase information disclosure [37,67]. In this case, the existence of the privacy paradox could be supported, since privacy concerns are found to be inconsistent with actual behaviour.

In addition, in the context of social media, the privacy paradox has often been studied in terms of the effect of privacy concerns on potential efforts to follow a privacy protective but nevertheless active use of social media. In other words, studies have been focusing mainly on potential privacy protection strategies, such as giving false personal information [68–70], configuring privacy settings [71], and deleting previously shared information [72], that people may apply in order to achieve a more cautious social media activity, in case they express concerns about their privacy. As such, studies seeking to understand the possibility of privacy concerns resulting in a merely passive use of social media (e.g., viewing information shared by others without sharing any information) or even a temporary termination of social media use (e.g., account deactivation) remain scarce [73].

A privacy paradox study based on both passive and active social media use is missing from current privacy literature and can be provided by the model of this article.

3.2.5. Summary of Privacy Paradox Explanations

The privacy paradox explanations are summarised in Table 2. However, the privacy paradox remains a complex phenomenon that has not been fully explained yet. First, current explanations consider only separate subsets of the problems and shortcomings that stand in the way of informed and rational privacy decisions, hence remaining incomplete [12]. Second, current explanations are based on studies that have used mainly cross-sectional approaches, thus neglecting the changes taking place over time.

Table 2. Privacy paradox explanations.

Explanation	Description
Rational risk assessment	
Privacy calculus	People perform a perfectly informed and rational cost-benefit analysis and decide to share their data only when the potential benefits of disclosure outweigh the expected privacy costs. However, people might still express concerns about their data being lost, resulting in the apparent inconsistency between expressed privacy concerns (or attitude) and actual behaviour.
Irrational risk assessment	
Incomplete information, bounded rationality, and decision biases	People compensate for limitations in information, time, and cognitive capabilities by using heuristics, which might still result in unexpected outcomes. Hence, the original intention or expressed attitude towards the behaviour might not be reflected in the actual behaviour.
Little to no risk assessment	
Social influence	People's expressed attitude is apparently echoing their unbiased opinion. However, people's actual behaviour is often affected by social factors. Hence, the expressed attitude is not necessarily reflected in the actual behaviour.

3.3. Privacy Obstacles

Over the years, privacy researchers have identified numerous problems and shortcomings, behind current explanations, that make informed and rational privacy decisions conceptually and practically demanding. These problems and shortcomings have been distilled into eight concrete privacy obstacles, which are also categorised into three groups based on how easy they are to be addressed with appropriate tools: (1) *solvable*, which seem more practical in nature and have the potential to be solved with appropriate tools, (2) *challenging*, which have the potential to be mitigated but exhibit aspects being likely unsolvable, and (3) *insuperable*, which feature social dimensions and seem unsolvable regardless of any tools made available [14].

The first solvable obstacle is *Timing and Duration*, which refers to the difficulty of estimating long-term costs. To make matters worse, the indefinite duration of the consent does not always give the option to revisit privacy decisions or even revoke consent at a future date. The second solvable obstacle is *Non-negotiability*, referring to the limited (often all-or-nothing) consent options offered by service providers. That is, either accepting the terms in full to be able to use the service or rejecting them and not use the service. The last solvable obstacle is *Scale*, which refers to the number of privacy decisions that individuals are supposed to make due to (1) the lengthiness and complexity of privacy policies and settings and (2) the number of different services one normally faces.

The first challenging obstacle is *Aggregation*, which refers to the data produced with analytic techniques from the data shared by individuals. In other words, data collecting entities aggregate openly expressed (e.g., photo sharing) and exhaust (e.g., website click-streaming) data and analyse it to reveal new —latent— data, which individuals are often not aware of. The second challenging obstacle is *Downstream Uses*, referring to unexpected flows of data to third parties, again often without awareness of the individuals involved, even though individuals may have consented to such data flows. Both Aggregation and Downstream Uses are mainly due to the apparent inability of individuals to be (1) properly informed of what exactly they are consenting to and (2) aware of the negative consequences such consent may have. Therefore, individuals are not able to determine for themselves when, how, and to what extent information about them is communicated to others [41,74].

The last challenging obstacle is *Cognitive Demands*, which refers to the limits of human decision-making ability.

The first insuperable obstacle is *Social Norm*, which refers to individual decisions being regulated by mass decisions. That is, the more people conform and use online services, the harder it becomes to deviate from the norm and not participate regardless of privacy preferences and concerns. Finally, the second insuperable obstacle is *Social Data*, referring to individual activities leaking —incidental— data about others (often without them being aware of the leak). Therefore, privacy can be affected by the choices of others, and the outcomes of data sharing decisions are not only private.

The eight privacy obstacles are summarised in Table 3.

Table 3. Privacy obstacles [14].

Obstacle	Description
Solvable	
Timing and Duration	Estimating costs is difficult due to timing of decisions and the typically unlimited duration of the consent.
Non-negotiability	The terms are not negotiable enough.
Scale	The cost-benefit analysis does not scale well to a large number of separate privacy decisions.
Challenging	
Aggregation	Data is aggregated and analysed to produce new data, leading to implicit disclosure of latent data.
Downstream Uses	Data flows to parties and purposes not foreseen at the time of consenting.
Cognitive Demands	The cognitive limitations of all human decision-making hamper cost-benefit analysis.
Insuperable	
Social Norm	Pressure to conform can strongly affect the decisions people make.
Social Data	Privacy decisions are framed as individual choices, but the data and the decisions can also affect others.

Relation of Privacy Paradox Explanations to Privacy Obstacles

The relation of privacy paradox explanations to the eight privacy obstacles is summarised in Table 4. First, the privacy calculus theory assumes that people make perfectly informed and rational privacy decisions, and it therefore neglects different conditions, such as incomplete information and bounded rationality, that affect privacy decision-making. The eight privacy obstacles essentially reveal the futility behind this assumption.

Second, incomplete information might result in inability to evaluate the potential benefits and costs of privacy decisions. The obstacles of Social Data, Aggregation, and Downstream Uses refer to the data sharing and processing practices that aggravate incomplete information. Similarly, bounded rationality might result in inability to make objectively right and unbiased decisions. The obstacles of Timing and Duration and Cognitive Demands refer to the limitations in both time and cognitive processing ability that aggravate bounded rationality. Furthermore, even if complete information and unbounded rationality were possible, they might still not suffice to prevent imperfect privacy decisions. The obstacles of Non-negotiability and Scale refer to the limitations in privacy control that aggravate boundary regulation efforts.

Finally, previous privacy paradox studies have used different terms, such as social theory [12] and social influence [13], to describe the social pressure that affects privacy decision-making. The obstacle of Social Norm refers to the same effect.

Table 4. Relation of privacy paradox explanations to privacy obstacles.

Explanation	Obstacle
Rational risk assessment	
Privacy calculus	The eight privacy obstacles reveal the futility of assuming a perfectly informed and rational cost-benefit analysis in privacy decision-making.
Irrational risk assessment	
Incomplete information, bounded rationality, and decision biases	Social Data, Aggregation, and Downstream Uses relate to issues that prevent access to complete privacy information.
	Timing and Duration and Cognitive Demands relate to issues that prevent objectively right and unbiased privacy decision-making.
	Non-negotiability and Scale relate to issues that prevent real choice within boundary regulation.
Little to no risk assessment	
Social influence	Social Norm refers to the social pressure that affects privacy decision-making as described by social influence.

4. System Dynamics Modelling

System dynamics is a methodology to understand how feedback loops, accumulations, and time delays between different factors affect the *behaviour of complex systems over time* [15]. System dynamics models can include both social and technical elements and are therefore a potent tool for studying complex sociotechnical systems, such as social media.

In system dynamics, *stock-flow diagrams* consist of variables, shown as named nodes, related by causal links, shown as arrows. *Stocks* are shown as rectangles and represent accumulations of either matter or information. *Flows* are shown as pipes and valves and regulate the rate of change of the stocks. Finally, intermediate variables between stocks and flows indicate *auxiliaries*, which essentially clarify the sequence of events that cause the flows to change the stocks.

The direction of a causal link indicates the direction of causation for a pair of variables: an independent variable (i.e., a cause) at the tail of the causal link and a dependent variable (i.e., an effect) at the head of the causal link. All causal links indicate that the dependent variable changes in the *same* direction as the independent variable unless they are labelled with a minus sign (−), in which case the dependent variable changes in the *opposite* direction. In addition, *delay* is the process by which an effect lags behind its cause in time, and it is shown by a causal link that is broken by parallel lines.

Finally, *feedback* is the process whereby an initial cause is changed on the basis of its effect, thereby forming a loop. Variables constituting feedback loops are at the same time both causes and effects. Feedback loops are either *reinforcing* (R), which amplify change, or *balancing* (B), which counteract and oppose change.

System dynamics has been used in studies from many different contexts, such as construction projects [75], product development [76,77], and safety critical organizations [78], but also for fields related to the topic of this article, including the attitude-behaviour gap [79] and the platform value creation process [80]. A common theme emerging from these studies is the trade-offs between the more gratifying future benefits of long-term goals and the less gratifying immediate benefits of short-term goals. Another theme is the means by which feedback loops and time delays hamper the best course of action [81] and therefore often result in imperfect decisions. For this reason, modelling tools, such as system dynamics, are useful in examining the unintended consequences of decisions.

In system dynamics, the modelling process involves five steps: (1) *problem articulation*, defining *reference modes* that illustrate the problem as a pattern of behaviour over time, (2) *formulation of a dynamic hypothesis*, aiming to explain the problematic behaviour shown in the reference modes in terms of the underlying feedback and stock-flow structure of the system, (3) *model development*, specifying the structure of the system, (4) *model testing and validation*, ensuring the validity of the model, and (5) *policy design*, recommending strategies

and structures for addressing the problem [15]. The application of these steps is described in the following sections.

5. Dynamic Model of Interdependencies between Privacy Obstacles and Social Media Adoption and Use

The modelling process begins with the problem articulation. The adoption of platforms is typically expected to follow an *S-shaped growth* pattern: initially, the number of users grows slowly in a positive acceleration phase; subsequently, the number of users grows exponentially; finally, the growth in users becomes slow again, but this time in a negative acceleration phase, until it ultimately stabilises [82]. For this reason, the privacy paradox in the context of social media is illustrated in this article using two reference modes: (1) an S-shaped growth of highly concerned users, who remain *passive* in the platform without sharing their data, illustrates a situation in which privacy concerns are consistent with actual behaviour, thus at least partially resolving the privacy paradox, and (2) an S-shaped growth of highly concerned users, who create platform content by *actively* sharing their data, illustrates a situation in which privacy concerns are inconsistent with actual behaviour, thus reflecting the privacy paradox. Using these two modes of dynamic behaviour, *the purpose of the model* is to explain how the decisions of people regarding adoption and use of social media are affected by the eight privacy obstacles (Figure 1).

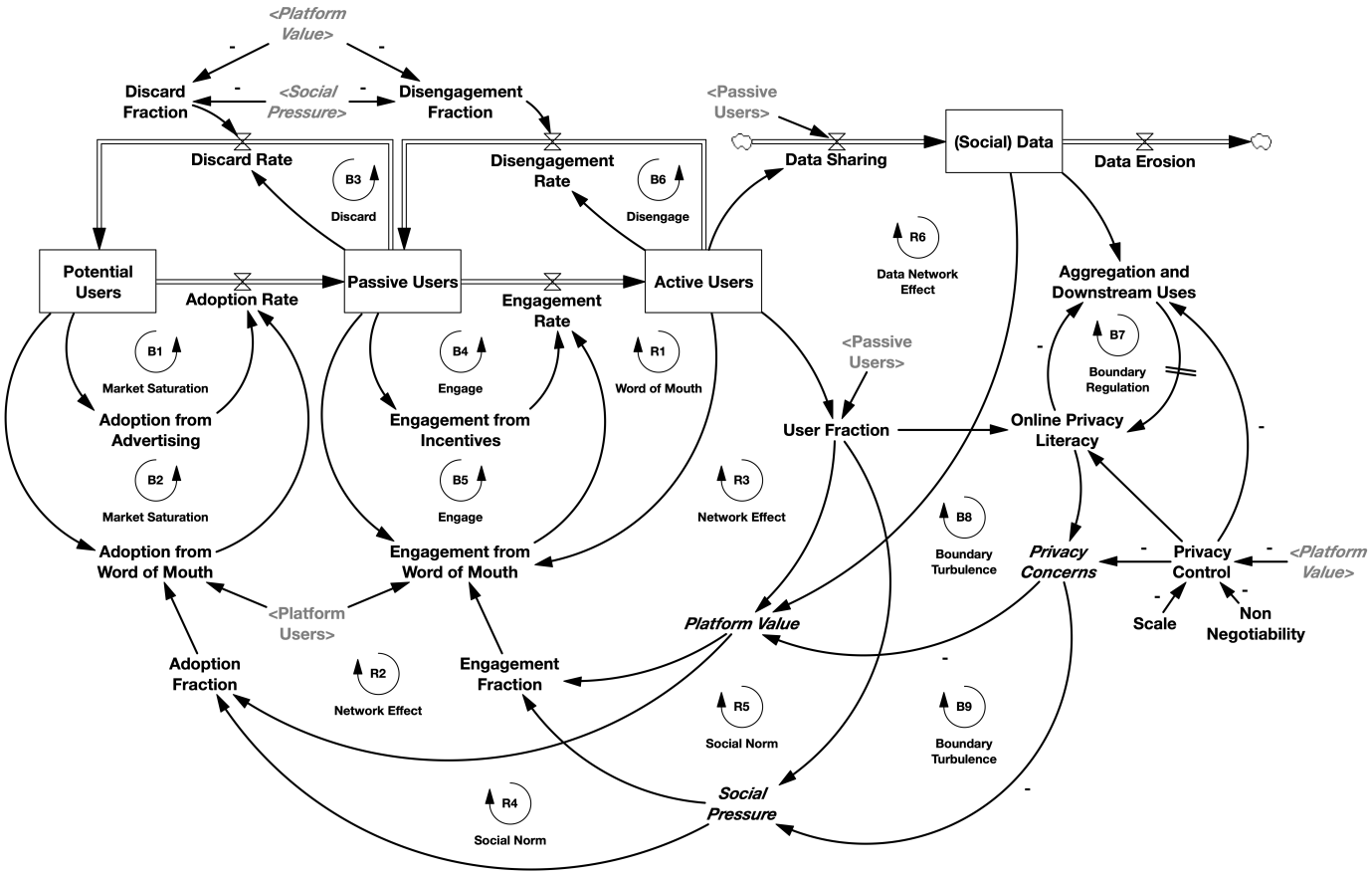

Figure 1. Privacy obstacles affecting the adoption and use of social media.

The second step in the modelling process is the formulation of a dynamic hypothesis. The Bass model of *innovation diffusion*, which describes the adoption of new products or services (over time) through advertising and word-of-mouth [83], is a widely used and well-established model in platform literature that can produce S-shaped growth patterns [46,80,82]. For this reason, the dynamic hypothesis guiding the model development is that by extending the feedback structure of the Bass model of innovation diffusion to

include the eight privacy obstacles, it is possible to produce the two modes of dynamic behaviour. Here, in addition to platform adoption, the model also considers platform use, and current users are disaggregated into passive and active users. Passive users are the platform's lurkers, who remain in the platform without engaging in data sharing. However, they do provide some basic amount of data required for opening their account, and they may also reveal part of their interests and habits by viewing the platform's content. Conversely, active users are the platform's content creators, who generate information by sharing their data.

5.1. Feedback Loops

The third step in the modelling process is the model development. The model consists of six reinforcing (R) and nine balancing (B) feedback loops.

Platform adoption (B1-3): The first feedback loops of the model relate to platform adoption. When the platform is launched, the initial number of users is zero, so the only source of adoption are external influences, such as advertising (B1: "Market Saturation"). When the first users enter the platform, the adoption rate increases through word-of-mouth (B2: "Market Saturation"). The advertising and word-of-mouth effects are largest at the start of the platform diffusion process and steadily diminish as the stock of potential users is depleted (B1-2: "Market Saturation"). Finally, passive users may decide to discard the platform and re-enter the stock of potential users (since they may be persuaded to adopt again in the future). In this case, the discard rate depends on the number of passive users, the net value of benefits minus costs they receive from the platform, and the social pressure towards platform adoption (B3: "Discard").

Platform engagement (R1, B4-6): The feedback loops related to platform engagement are similar to these of platform adoption. In the beginning, the initial number of active users is zero, which implies zero user interactions. As a result, platform activity emerges from the incentives used by the platform to encourage the creation of content (B4: "Engage"). Incentives can be implicit, such as emotional rewards of belonging to a community, or explicit, such as monetary rewards. When the first users become active in the platform, the engagement rate increases through word-of-mouth (R1: "Word of Mouth"). The incentives and word-of-mouth effects are largest at the start of the engagement process and steadily diminish as the stock of passive users is depleted (B4-5: "Engage"). Finally, active users may decide to stop engaging in data sharing and become passive. In this case, the disengagement rate depends on the number of active users, the net value of benefits minus costs they receive from the platform, and the social pressure towards platform engagement (B6: "Disengage").

Network effect and Social Norm (R2-5): Network effect and Social Norm are each represented by two reinforcing feedback loops. As the number of *users* grows, platform value (i.e., the difference of benefits and costs) increases, thus inducing further platform adoption (R2: "Network Effect") and use (R3: "Network Effect") [84]. At the same time, the social pressure towards platform adoption and use becomes stronger and consequently harder to deviate from. As a result, more potential users conform and adopt the platform (R4: "Social Norm"), and more passive users conform and become active in the platform (R5: "Social Norm") [3,85].

Data network effect (R6): The feedback loop related to data network effect is similar to these of network effect. As the amount of *data* increases, platform value increases, thus inducing further platform adoption and use (R6: "Data Network Effect"). The operation of data sharing platforms, such as social media, describes a process that takes accumulated data as an input and produces value as an output. In other words, the data shared by users accumulates to the platform, and it enables users to interact in a valuable manner [86], which becomes one of the core motivations to adopt and use the platform and also the chief denominator to measure changes in value across the platform [87].

Boundary regulation (B7): Boundary regulation [44] is represented by one balancing feedback loop. The more knowledgeable users become about privacy, the platform's data

processing practices, and potential privacy protection strategies, the better users become able to control whether and how their data can be aggregated and analysed (Aggregation) or shared with third parties (Downstream Uses) (B7: "Boundary Regulation").

Boundary turbulence (B8-9): The final feedback loops of the model relate to boundary turbulence [44]. Inadequate privacy control options offered by the platform result in failure or inability of users to control their data and therefore higher privacy concerns. The higher the concerns, the less the value that users receive from the platform (B8: "Boundary Turbulence") and the less the social pressure that users create towards platform adoption and use (B9: "Boundary Turbulence").

5.2. Effect of Privacy Obstacles on Feedback Loops

This section summarises the effect of each privacy obstacle on the feedback loops, and it therefore addresses RQ1: *How do the privacy obstacles affect people's privacy behaviour over time?*

Social Data: The data shared by users accumulates to the platform, and it may contain information not only about themselves but also directly reveal information about others. Social Data may be shared intentionally, such as sharing photos of other people for celebratory or social criticism and humiliation purposes, or unintentionally, such as sharing photos of public places that include other people in the background. On one hand, perfect awareness of Social Data seems practically impossible, since it might be shared in non-transparent manners (e.g., private messaging or closed user groups) or by unfamiliar individuals. On the other hand, Social Data is shared by and for users, and it enables users to engage in valuable interactions. Hence, the obstacle of Social Data refers to the users' data sharing practices that aggravate incomplete information, but it also increases platform value, thus inducing further platform adoption and use.

Aggregation and Downstream Uses: Data erosion indicates the value of old data that gradually decreases. However, as long as the accumulated data remains accurate and timely, the platform is likely to keep processing it further. First, the platform analyses the data shared by users with the purpose to reveal additional information about them (Aggregation) [88]. Second, data shared by users often reaches third parties outside the platform, and conversely data shared on other platforms often reaches the current platform, thus providing more data for the service to analyse (Downstream Uses) [88]. On one hand, perfect awareness of Aggregation and Downstream Uses seems practically impossible, since most platforms are typically intentionally vague about them. On the other hand, over the last decade, numerous practices of Aggregation and Downstream Uses by some market leading platforms have been brought to the fore [89–92]. In addition, light on complex privacy policies has been shed, and the switching to privacy respecting platforms has been encouraged [93]. Hence, the obstacles of Aggregation and Downstream Uses refer to the platform's data processing practices that aggravate incomplete information, but they also determine Online Privacy Literacy, since the existence and negative consequences of such practices have been repeatedly communicated even without relevant intricate details.

Online Privacy Literacy: Privacy information from both informal (e.g., media, activists, peer groups) and formal (e.g., training programs) sources [94] promotes the understanding of potential negative consequences related to platform participation and data sharing, and it therefore contributes to fostering *online privacy literacy*, which "encompasses an informed concern for privacy and effective strategies to protect it" [95]. Trepte et al. elaborate that "online privacy literacy may be defined as a combination of factual or declarative ('knowing that') and procedural ('knowing how') knowledge about online privacy. In terms of declarative knowledge, online privacy literacy refers to the users' knowledge about technical aspects of online data protection, and about laws and directives as well as institutional practices. In terms of procedural knowledge, online privacy literacy refers to the users' ability to apply strategies for individual privacy regulation and data protection" [96]. Hence, as users become more literate about privacy, the platform's data processing practices, and potential privacy protection strategies, they become more able to

control their data Aggregation and Downstream Uses. In addition, higher numbers of users (i.e., platforms with larger installed user bases) are more likely to entail higher privacy risks and therefore increase the efforts to foster online privacy literacy.

Boundedly rational adoption and use of social media: The behaviour of potential and current users depends on the subjective and biased assessment of information that is available to them at a given point in time. In other words, potential and current users are not able to have perfect foresight of how negative consequences will develop, and they do not necessarily learn about, understand, and react to negative consequences. As a result, they make their decisions regarding platform adoption, discard, engagement, and disengagement based on their *perception* of platform value and social pressure to them, depending on their concerns about negative consequences that are apparent to them at the time (i.e., negative consequences of the past).

Timing and Duration: Even if insignificant short-term negative consequences related to platform participation and data sharing are apparent, it can take time for privacy risks to materialise into more significant negative consequences. In this case, users may concentrate on negative consequences that are less significant and present, thereby underestimating and caring less about these that are more significant but also more distant in time (i.e., temporal discounting) [97]. As a result, users may decide (relying on heuristics [50,51]) that the immediate benefits of disclosure outweigh apparent and insignificant short-term negative consequences [52], hence becoming only gradually concerned about privacy as more significant negative consequences develop and start to be realised over time. The higher the concerns, the less the value that users receive from the platform and the less the social pressure that users create towards platform adoption and use. Hence, the obstacle of Timing and Duration, represented by a delay in the causal link between Aggregation and Downstream Uses and Online Privacy Literacy, refers to privacy concerns that are based on present rather than future negative consequences, and it therefore aggravates boundedly rational decisions regarding platform adoption, discard, engagement, and disengagement.

Cognitive Demands: Even if privacy information is made readily available, online privacy literacy is a cognitive process [96]. That is, users may be reluctant to become literate [48,50] and consciously choose to ignore a certain piece of information, in case the costs of learning are disproportionate to the potential benefits of disclosure (i.e., rational ignorance theory) [98]. For example, users may consider that the costs (e.g., loss of time or cognitive effort) of learning about potential negative consequences by reading complex privacy policies in their entirety outweighs potential negative consequences per se. As a result, users may decide (relying on heuristics [50,51]) that the benefits of adopting and using social media outweigh the costs of learning [52]. Moreover, even if users are not reluctant to become literate, they might still not be able to make proper sense of the negative consequences they learn about [48]. Here, the model assumption is that becoming more literate about potential negative consequences increases awareness of privacy risks, thereby leading to a heightened sense of vulnerability and higher privacy concerns [96,99–101]. The higher the concerns, the less the value that users receive from the platform and the less the social pressure that users create towards platform adoption and use. Hence, the obstacle of Cognitive Demands, represented by the italicised Privacy Concerns, Platform Value, and Social Pressure, refers to privacy concerns that are based on subjective and biased assessment of negative consequences, and it therefore aggravates boundedly rational decisions regarding platform adoption, discard, engagement, and disengagement.

Non-negotiability and Scale: Even if users become literate, they might still not be able to utilise their knowledge and control their data due to inadequate privacy control options offered by the platform. First, the platform might not negotiate the processing of data (Non-negotiability) [74]. Second, the platform's privacy policy and settings could be lengthy and complex (Scale) [48]. The less negotiable the terms of service and the more lengthy and complex the privacy policies and settings, the less cognitive effort per option users can invest in controlling their data. Hence, the obstacles of Non-negotiability and Scale refer to the limitations in privacy control that aggravate boundary regulation efforts. Privacy

Control determines both Online Privacy Literacy, since privacy protection strategies are developed based on available options, and Privacy Concerns, since users' perception that potential processing of their data is conducted fairly (i.e., procedural fairness) [47], and that there will be no significant negative consequences related to platform participation and data sharing, depends also on available options. Here, the model assumptions are that (1) becoming more literate about and having to choose from inadequate privacy control options reduces response efficacy (i.e., users' belief that available options are effective in privacy protection), thereby exacerbating the sense of vulnerability and privacy concerns [102,103], and (2) becoming more literate about and having to choose from adequate privacy control options increases self-efficacy (i.e., users' belief in their own ability to protect their privacy), thereby leading to a heightened sense of safety and lower privacy concerns [101,104]. As such, the model takes also into consideration the possibility of a *control paradox*, by which users are more likely to disclose even more private information if they (believe that they) are able to effectively control their information [102].

Boundedly rational boundary regulation: Both privacy theories by Westin [41] and Altman [42] discuss access control or regulation to the self. In addition, CPM theory implies that controlling personal data should be possible [44]. Thus, data analysis (Aggregation) and data flows to third parties (Downstream Uses) are affected by the privacy control options offered by the platform. However, even if adequate options are made readily available, boundary regulation is a cognitive process. That is, users may concentrate their time and entire cognitive, affective, and physical resources (i.e., cognitive absorption) [105,106] on obtaining concrete and immediate benefits from adopting and using social media and therefore care less about controlling their data Aggregation and Downstream Uses [48], hence being more likely to disclose even more private information [107] (i.e., another control paradox possibility [102]). As such, boundary regulation efforts are assumed to be boundedly rational. Failure or inability of users, resulting from inadequate available options (Non-negotiability and Scale) or bounded rationality (Timing and Duration and Cognitive Demands), to control (1) whether the platform and third parties can access their data (linkage), (2) the amount of their data to which the platform and third parties can have access (permeability), and (3) the extent of their data Aggregation and Downstream Uses (ownership) indicates what Petronio refers to as boundary turbulence (B8, B9: "Boundary Turbulence") [44].

The causal dependencies of the eight privacy obstacles are summarised in Table 5. The obstacles can be categorised into three groups based on their effect on informed and rational privacy decision-making in the context of social media: (1) *incomplete information*, which prevent perfectly informed evaluation of potential benefits and costs, (2) *bounded rationality*, which prevent perfectly rational assessment of potential benefits and costs, and (3) *real choice limitations*, which prevent perfectly thorough analysis of potential benefits and costs.

5.3. Model Testing and Validation

The fourth step in the modelling process is the model testing and validation. To ensure the validity of the model, with respect to the purpose of the model presented in Section 5, the model structures have been formulated based on current platform and privacy literature. The model includes a social media platform that is modelled *endogenously*, meaning that the dynamics of the variables constituting the feedback structure of the platform are generated by the interactions among these variables themselves. The core feedback structure of the platform has been formulated by extending the Bass model of innovation diffusion [83] and the platform adoption model of Ruutu et al. [80].

Table 5. Causal dependencies of privacy obstacles.

Obstacle	Description	Causal Dependencies
Incomplete information		
Social Data	The data shared by users may directly reveal information about others.	Social Data is affected by Data Sharing and affects Aggregation, Downstream Uses, and Platform Value.
Aggregation	The platform analyses the data shared by users with the purpose to reveal additional information about them.	Aggregation and Downstream Uses are affected by Social Data, Privacy Concerns, and Privacy Control. In addition, they affect and are also affected by Online Privacy Literacy.
Downstream Uses	Data shared by users often reaches third parties outside the platform, and conversely data shared on other platforms often reaches the current platform.	
Bounded rationality		
Timing and Duration	Privacy concerns gradually rise as more significant negative consequences develop and start to be realised over time.	Timing and Duration affect Online Privacy Literacy, while Cognitive Demands affect Privacy Concerns, Platform Value, and Social Pressure.
Cognitive Demands	Time and cognitive resources are limited and invested mostly in obtaining concrete and immediate benefits rather than learning about, understanding, and reacting to negative consequences.	
Real choice limitations		
Social Norm	As the number of users grows, more potential users conform, adopt, and use the platform.	Social Norm affects Adoption, Discard, Engagement, and Disengagement Fraction.
Non-negotiability	The platform might not negotiate the processing of data.	Non-negotiability and Scale affect Privacy Control.
Scale	The platform's privacy policy and settings could be lengthy and complex.	

In addition, the model assumptions behind the interdependencies between the eight privacy obstacles and the social media platform are based on current privacy literature. Social Data, Aggregation and Downstream Uses, Online Privacy Literacy, and Privacy Concerns are variables that are determined by the actors represented in the model, particularly potential and current users, and are modelled endogenously. By contrast, Non-negotiability, Scale, and Privacy Control are modelled as exogenous variables.

Disaggregating current users into passive and active users allows for identifying the fraction of current users whose privacy concerns are consistent with actual behaviour towards social media use. For example, potential users may adopt the platform, but platform adoption is not necessarily an indication of platform activity and data sharing, since highly concerned users may eventually follow a merely lurking approach to using the platform or even take a break from the platform. In this case, the existence of the privacy paradox can be challenged, as discussed in Section 2, even if the platform exhibits high numbers of current users. In other words, high privacy concerns resulting in high numbers of passive users can challenge the existence of the privacy paradox, since privacy concerns are consistent with the decision to lurk and not engage in data sharing. Conversely, high numbers of active users regardless of high privacy concerns can support the existence of the privacy paradox,

since privacy concerns are inconsistent with the decision to create content by engaging in data sharing.

6. Analysis

This section addresses RQ2: *How do the privacy obstacles help understand the privacy paradox?*

People adopt and use social media in order to satisfy different needs and to achieve particular gratifications, ideally without negative consequences, such as loss of privacy. However, people also encounter problems and shortcomings (i.e., privacy obstacles), which exist within both social media and the society at large, and which entail privacy risks that may lead to negative consequences. *Platform value* indicates the net value resulting from the benefits (i.e., gratifications) minus the costs (i.e., negative consequences) that people receive when using social media.

When the first users become active in the platform, gratifications (R2-3, R6) kick off and (rapidly) increase, thereby dominating negative consequences (B8-9), which typically (initially) come across as minor (Figure 2). The model illustrates that platform value is determined by three effects, two positive and one negative. The gratifications achieved by social media adoption and use are represented by the two positive effects on platform value. The first positive effect implies that *higher numbers of users tend to generate higher gratifications by satisfying needs like connecting with peers and family*, thus increasing platform value (R2-3) and inducing further platform adoption (B1-2) and use (B4-5, R1). Similarly, the second positive effect implies that *larger amounts of shared data tend to generate higher gratifications by satisfying needs like seeking and sharing information*, thus increasing platform value (R6) and inducing again more potential users to adopt (B1-2) and use (B4-5, R1) the platform.

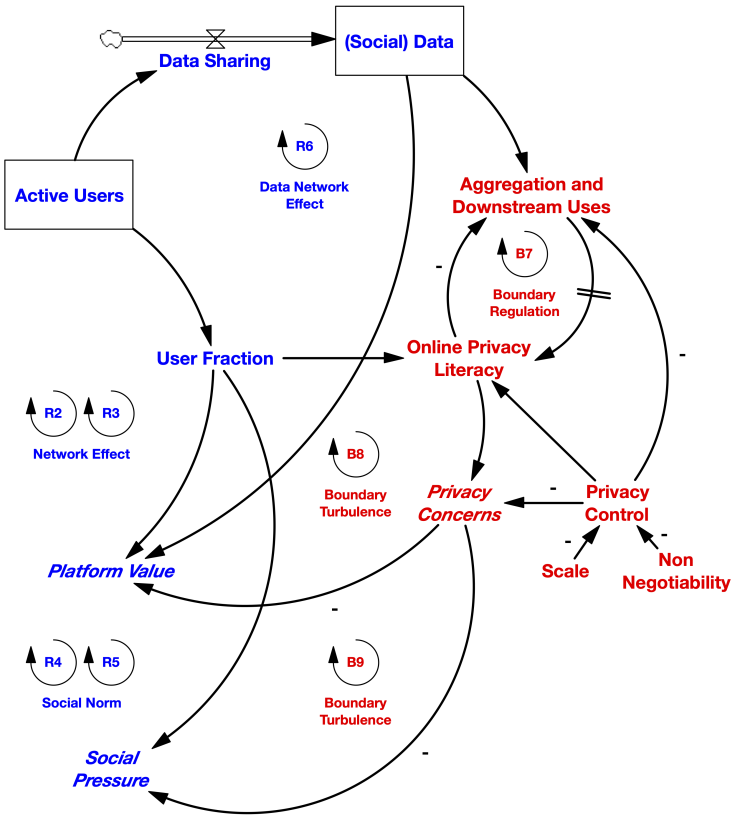

Figure 2. Gratifications (R2-3, R6), which are also reinforced by social pressure (R4-5), kick off early and dominate even major negative consequences (B8-9) that become apparent over time.

The two positive effects on platform value are reinforced by *social pressure*. While generating higher gratifications, *higher numbers of users tend to also generate stronger normative platform participation and data sharing behaviour*, thus increasing social pressure (R4-5) and

influencing more potential users to conform and be connected with the admired peer groups (rather than deviate and be sanctioned with attention deprivation and peer group exclusion). As such, the adoption and use of social media is often driven by the need to steer clear of social stigmas and to achieve a sense of safety, which may be considered an additional benefit along with gratifications. Hence, the obstacle of Social Norm (R4-5) reinforces gratifications (R2-3, R6), thus inducing further platform adoption (B1-2) and use (B4-5, R1).

By contrast, the negative consequences of social media adoption and use are represented by the negative effect on platform value. While generating higher gratifications, *larger amounts of shared data tend to also generate larger negative consequences, such as (1) leaking larger amounts of information (Social Data), (2) deducing larger amounts of implicit information (Aggregation), and (3) moving larger amounts of information to new parties (Downstream Uses)*. However, not all negative consequences are (immediately) apparent, and even as some could become apparent in the short term (Timing and Duration), they typically (initially) come across as minor and are therefore either ignored (often due to an illusory sense of disproportionately high gratifications) or underestimated (often due to an illusory sense of adequate privacy control options [102]) (Cognitive Demands). As such, privacy concerns (initially) remain low, while gratifications (rapidly) increase and negative consequences continue to (slowly) develop. Hence, the privacy obstacles hamper the realisation of (all) negative consequences (B8-9), thus reducing the motivation for platform discard (B3) and disengagement (B6).

As gratifications (rapidly) increase and negative consequences continue to come across as minor, the feedback loops related to network effect (R2-3), data network effect (R6), and Social Norm (R4-5) dominate the feedback loops related to boundary turbulence (B8-9). For this reason, the feedback loops related to adoption (B1-2) and engagement (B4-5, R1) ultimately dominate the feedback loops related to discard (B3) and disengagement (B6) (Figure 3).

In the early phase of platform adoption and use, gratifications (R2-3, R6) have already grown too high, thereby dominating even major negative consequences (B8-9) that become apparent over time. Data sharing determines at the same time, but crucially at different rates, both social media gratifications and negative consequences. Following the early phase of platform adoption and use, privacy concerns gradually rise as the apparent negative consequences become more significant (Timing and Duration), hence coming into larger conflict with earlier generated gratifications and also reversing the belief that fixed terms (Non-negotiability) and complex privacy policies (Scale) are effective in privacy protection. However, even major negative consequences (B8-9) can be neglected often due to intense concentration (Cognitive Demands) on gratifications (R2-3, R6), which are also reinforced by social pressure (R4-5).

As high gratifications continue to be prioritised over major negative consequences, the feedback loops related to network effect (R2-3), data network effect (R6), and Social Norm (R4-5) continue to dominate the feedback loops related to boundary turbulence (B8-9). For this reason, although the feedback loops related to discard (B3) and disengagement (B6) become stronger, they continue to be dominated by the feedback loops related to adoption (B1-2) and engagement (B4-5, R1).

The privacy paradox emerges if users choose to start or continue using the platform when platform value decreases (i.e., when negative consequences come into larger conflict with gratifications). However, the exact threshold value depends also on the sensitivity of users to privacy concerns (i.e., it depends on which of e.g., Westin's segments the users belong to), as this sensitivity determines the gratifications that users are willing to forego in order to achieve their desired privacy level.

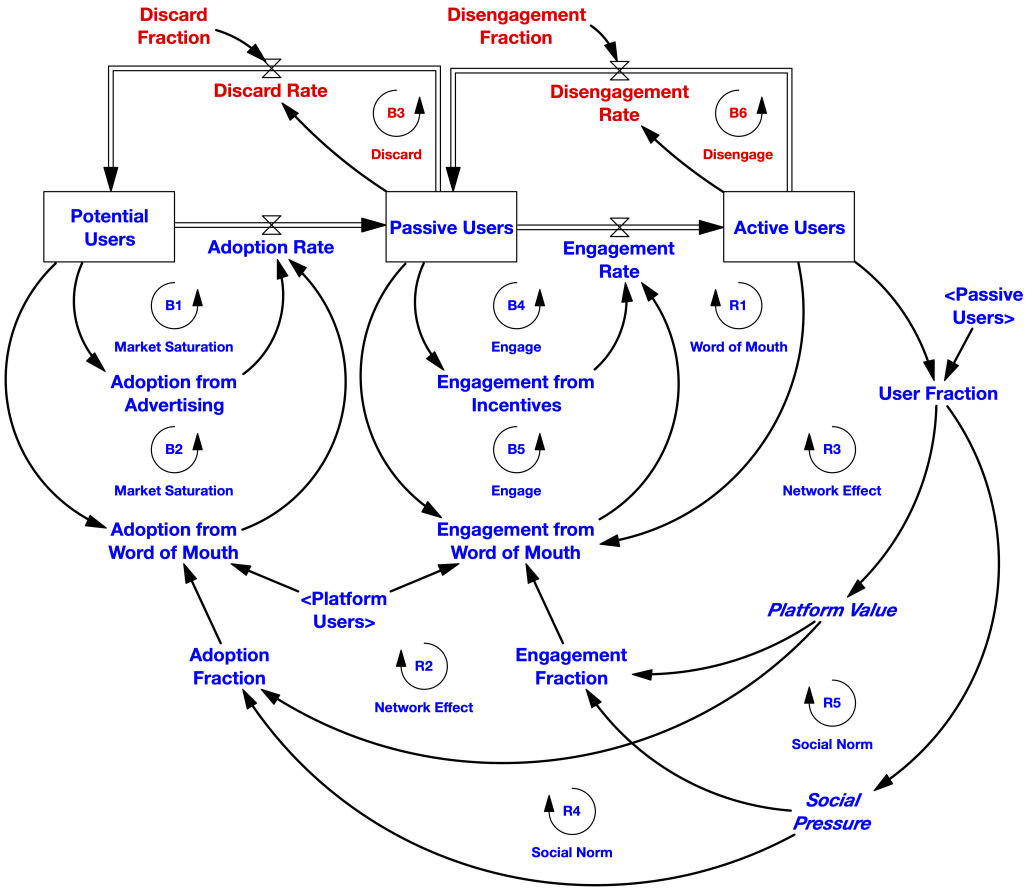

Figure 3. Social media adoption (B1-2) and engagement (B4-5, R1) dominate social media discard (B3) and disengagement (B6).

Users are less likely to enter into a situation that demonstrates a clear paradox. Rather, *the privacy paradox can emerge as negative consequences become apparent over time* (i.e., users need to be aware of the negative consequences for the paradox to exist). Hence, paradoxical situations in social media can often be explained by the inability of users to adequately account for the negative consequences in the beginning. As such, by the time negative consequences become apparent, and therefore the paradox emerges, gratifications and social pressure have grown too high for users to discard the platform (i.e., the boiling frog syndrome [16]). One potential real-life example resembling this case could be the Facebook—Cambridge Analytica scandal [108], which caused only a temporary decline in Facebook's daily and monthly EU active users [109,110]. At the same time, the monthly active users of WhatsApp and Instagram, which are owned by Facebook, have been steadily increasing [111,112].

Conversely, major short-term negative consequences (B8-9) are more likely to dominate gratifications (R2-3, R6) (Figure 4). In the early phase of platform adoption and use, when gratifications are low to be intensely concentrated on, any publication of massive (1) leaks of information (Social Data), (2) deductions of implicit information (Aggregation), and (3) movements of information to new parties (Downstream Uses) is less likely to be ignored or underestimated (Cognitive Demands). As such, negative consequences are prioritised, privacy concerns rise, and gratifications remain low.

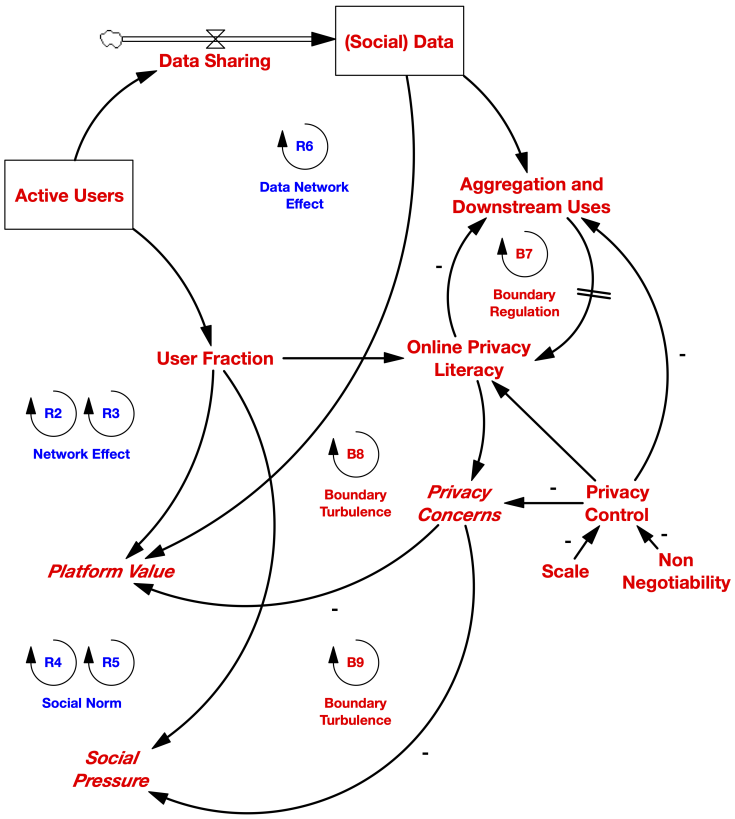

Figure 4. Major short-term negative consequences (B8-9), which are less likely to be ignored or underestimated, dominate low gratifications (R2-3, R6).

As major short-term negative consequences become disproportionate to low gratifications and inadequate privacy control options, the feedback loops related to boundary turbulence (B8-9) dominate the feedback loops related to network effect (R2-3), data network effect (R6), and Social Norm (R4-5). For this reason, the feedback loops related to discard (B3) and disengagement (B6) ultimately dominate the feedback loops related to adoption (B1-2) and engagement (B4-5, R1) (Figure 5).

Users are more likely to eventually discard the platform when they start to realise the negative consequences in the beginning, thus resolving the privacy paradox. One potential real-life example resembling this case could be Google Buzz, which was introduced in 2010 with the aim to rival Facebook. However, shortly after being launched, Google Buzz faced serious legal issues due to poor privacy practices [113]. As a result, it was discontinued and superseded by Google+, which was also terminated in 2019 mainly due to low user engagement [114].

Theoretically, the opposite development (i.e., a clear paradox being dissolved over time) is less likely to emerge in real life, as this would require that data Aggregation and Downstream Uses are either reduced by the platform, to which such practices are immensely valuable to consider reducing, or controlled by users, to whom the privacy control options offered by the platform are typically inadequate.

Hence, the boiling frog explanation, by which the privacy paradox emerges only after users have already started using the platform, is a key finding of this article that cannot be provided using only conventional cross-sectional approaches, thus requiring a process theory, such as system dynamics, that also takes into account the time element.

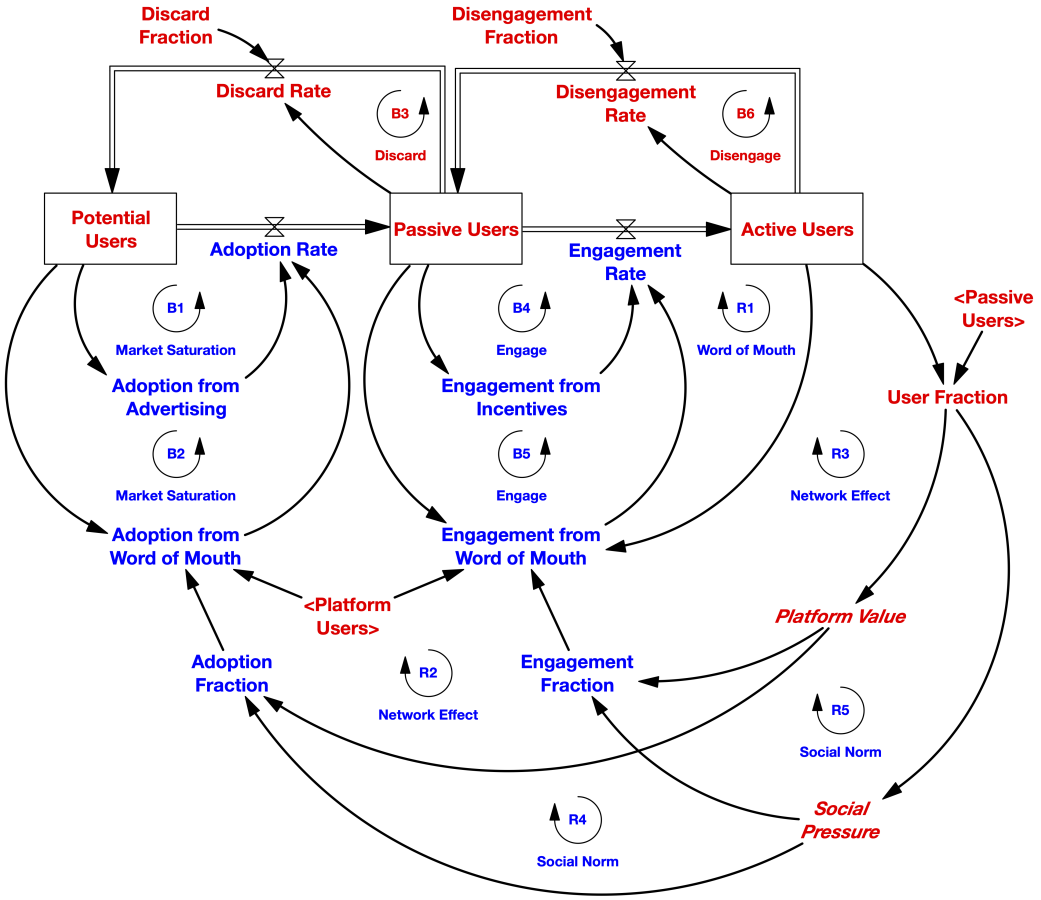

Figure 5. Social media discard (B3) and disengagement (B6) dominate social media adoption (B1-2) and engagement (B4-5, R1).

7. Discussion

The modelling process ends with the policy design. The boiling frog explanation highlights that users can arrive in a privacy paradox due to their limited ability to adequately account for the negative consequences of adopting and using social media. However, by addressing the privacy obstacles with appropriate tools, it may be possible to improve cost-benefit analysis in social media and therefore also reduce the extent of the privacy paradox.

7.1. Towards Informed Cost-Benefit Analysis

First, by addressing the obstacles of Social Data, Aggregation, and Downstream Uses, it may be possible to improve misinformed cost-benefit analysis in social media. However, *Social Data* makes privacy dependent on the decisions of others. Privacy preferences among users can be contradictory, and therefore data sharing gratifications may, from an individual perspective, outweigh the negative consequences imposed on others. Hence, Social Data seems an inherently unsolvable obstacle regardless of any tools made available.

On the other hand, although Aggregation and Downstream Uses may also seem likely impossible to be fully addressed, they might still be mitigated by increasing awareness [96] and providing transparency [115], respectively. First, becoming literate about potential negative consequences ex ante, before data is shared, could increase awareness of privacy risks, such as the production of latent data (*Aggregation*), which is possible only ex post, after data is shared. Increasing awareness of privacy risks could result in a better-informed concern for privacy and therefore a well-informed evaluation of negative consequences. However, due to the fact that negative consequences are moving targets, the evaluation of negative consequences cannot always be highly accurate. Nevertheless, even a coarse evaluation based on valid available information is likely to be more accurate compared to

using heuristics [96]. Second, as long as *Downstream Uses* refer to the data flows that are consented to by users, thus excluding cases of e.g., surveillance and data leaks, they could still be traced and eventually visualised. As such, abstract and complex data flows, which may seem ambiguous and confusing, could be translated into comprehensible graphical representations, from which useful insights could be pulled more efficiently (i.e., sense-making). However, the data industry includes structural constraints, such as opaque business practices and analytical layers, which separate data sources from data uses and therefore limit the transparency of data flows [115].

Hence, a perfectly informed cost-benefit analysis in social media seems practically impossible mainly because of the inability to foresee incidental data leaks (Social Data). However, highlighting the privacy risks of latent data (Aggregation) and visualising the flows of data to new parties (Downstream Uses) could provide useful information related to the costs of adopting and using social media. The more knowledgeable users become about data Aggregation and Downstream Uses, the better users become able to evaluate and reduce the negative consequences of such practices. As a result, the extent of the privacy paradox could also be reduced.

7.2. Towards Rational Cost-Benefit Analysis

Second, by addressing the obstacles of Timing and Duration and Cognitive Demands, it may be possible to improve irrational cost-benefit analysis in social media. On one hand, *Timing and Duration* might be mitigated by enabling unambiguous, informed, and revocable consent. Highlighting potential negative consequences ex ante, before consent is given, could increase awareness of privacy risks, such as the production of latent data (Aggregation) and the flows of data to new parties (Downstream Uses), which are possible only ex post, after consent is given, thereby reducing the timing issue. In addition, nudges to revisit privacy decisions and prompts to revoke consent could mitigate privacy risks that have not been taken into account, thereby reducing the duration issue. Nevertheless, nudges and prompts could also likely be just another forced click of an 'agree' button without much thought [74].

On the other hand, *Cognitive Demands* might be mitigated by making privacy decisions less demanding. On-time provision of relevant privacy information in a comprehensible format could reduce the time or cognitive effort required to become literate. However, converting now-opaque negative consequences into transparent ones could ultimately make each decision even more complex. In this case, one potential solution could be to change the nature of privacy decisions. That is, instead of considering each decision separately, several related decisions (e.g., consents for similar services) could be gathered under one well-considered decision.

Hence, a perfectly rational cost-benefit analysis in social media seems practically impossible mainly because of limitations in both time (Timing and Duration) and cognitive processing ability (Cognitive Demands). However, timely presentation of the upcoming collection, processing, and dissemination of data in the consent process (Timing and Duration) could promote a well-reasoned assessment of privacy risks. In addition, reversing privacy decisions (Timing and Duration), by re-evaluating, updating, and revoking consent, could mitigate irrational, negligible, or no assessment of privacy risks. Finally, simplifying privacy decisions (Cognitive Demands) could reduce the cognitive effort in the assessment of privacy risks. By enabling unambiguous, informed, and revocable consent when making privacy decisions, in addition to simplifying privacy decisions, it may be possible to improve misperceptions of information. As a result, the extent of the privacy paradox could also be reduced.

7.3. Towards Thorough Cost-Benefit Analysis

Finally, by addressing the obstacles of Social Norm, Non-negotiability, and Scale, it may be possible to improve incomplete cost-benefit analysis in social media. However, *Social Norm* makes analysis of potential benefits and costs to be driven by the need to

achieve conformity with the admired peer groups [116]. As such, people may neglect privacy concerns in order to reap the benefits of belonging to a community, since the costs (e.g., social stigmas) of being excluded from the community are undesirable [11]. In addition, people may engage in data sharing because this is an implicit rule of belonging to a community [117]. In this case, although the potential costs of data sharing may have been *abstractly* analysed, the concrete and immediate benefits of belonging to a community outweigh the abstract and long-term costs of data sharing [12]. Hence, Social Norm seems an inherently unsolvable obstacle regardless of any tools made available.

On the other hand, there seems to be no fundamental hurdle for (1) increasing the limited negotiating power over the terms of service (*Non-negotiability*) and (2) reducing the cognitive effort per option in configuring privacy settings (*Scale*). First, as long as Non-negotiability refers to the limited bargaining power of each user against social media, *collective action* from users could be taken in order to leverage the dependence of social media on users as data sources. Establishing some kind of a coordinating entity between users and social media could at least affect the power balance of the situation, and it could ideally give users the ability to utilise their knowledge and choose whether or not to consent to the terms under which their data can be collected and processed. As such, the belief that loss of privacy in social media is a situation that must be accepted and learned to live with (i.e., learned helplessness) [118], which often leads to a state of resignation about boundary regulation [73], could also be reversed. However, it seems safe to assume that the coordinating entity could also leverage its position for its own benefit, which may or may not align with the interests of users. Second, although Scale may seem an overwhelming task, it could be argued that it is not a problem of principle, but it is largely due to the means of implementing boundary regulation in practice. Clarifying privacy policies and simplifying privacy settings could eventually make cost-benefit analysis more manageable. Simplification of privacy settings could be achieved by simplifying each setting individually, gathering several low-level settings under one higher-level setting, or addressing several similar services at once. As such, feelings of exhaustion, resignation, and even cynicism towards privacy (i.e., privacy fatigue) [119], which are caused when the lengthiness and complexity of privacy policies and settings exceed the abilities and limits of a person [73], could also be reduced. Using automation and aides for highlighting important information within privacy policies and for recommending privacy settings configuration based on privacy preferences could work in this manner. However, practical questions remain about whether or not it is possible to achieve an extent of clarity and simplification that will satisfy expectations of users while complying with privacy regulation requirements [120,121].

Hence, a perfectly thorough cost-benefit analysis in social media seems practically impossible mainly because of individual decisions being regulated by mass decisions (Social Norm). However, having a say over the terms of service (Non-negotiability) could give the ability to play the cost-benefit analysis cards right (even if the costs have been abstractly analysed) in controlling whether and how personal data can be aggregated and analysed (Aggregation) or shared with third parties (Downstream Uses). In addition, clarifying privacy policies and simplifying privacy settings (Scale) could reduce the cognitive effort per option in controlling personal data. By outsourcing negotiations and applying privacy preferences with minimal human intervention, it may be possible to reduce the gap between actually achieved and desired privacy levels. As a result, the extent of the privacy paradox could also be reduced.

7.4. Studying Privacy with System Dynamics

Methodologically, the article demonstrates the potential of system dynamics as a tool for analysing privacy behaviour. The added value of using system dynamics for this analysis is that it allowed for building on existing privacy knowledge in order to (1) formulate the feedback loops related to Social Norm (R4-5), boundary regulation (B7), and boundary turbulence (B8-9) and (2) identify the effect of the eight privacy obstacles on these loops. A privacy paradox explanation based on feedback loops in general, and specifically on

the feedback loops that drive the decisions of people regarding adoption and use of social media, is missing from current privacy literature. Explanations that consider feedback loops are important, as humans typically misperceive the effects of feedbacks and delays in complex sociotechnical systems, such as social media. Hence, the original intention or expressed attitude (i.e., goals and wishes) towards the behaviour might not be reflected in the actual behaviour [61,62].

In addition, system dynamics allowed for examining the privacy paradox in a *dynamic* manner. In other words, the effect of the eight privacy obstacles on the feedback loops of the model does not remain static but rather changes over time. For this reason, the privacy paradox may either not emerge or emerge but vary in extent, thereby being more or less severe, at different points in time.

7.5. Directions for Future Research

In this article, a qualitative system dynamics model is used to illustrate multiple feedback loops that need to be considered for understanding the privacy paradox in the context of social media. The article's novel methodological approach to the privacy paradox opens up several fruitful avenues for future research.

First, a natural next step would be to develop the qualitative model into a fully fledged simulation model. While a qualitative model is useful in its own right for understanding causal dependencies, a quantitative simulation model would be useful in illustrating in more detail the complex behaviour over time that can result from the interaction of multiple feedback loops and time delays related to the adoption and use of social media.

Second, the model could be developed further to include a more fine-grained analysis of the diversity of privacy concerns and personal information [12]. In this regard, privacy segmentation, such as Westin's [45], could be used to divide people based on their privacy preferences. First, fundamentalists could be modelled to realise negative consequences faster (i.e., short delay) and interpret them as even worse, thus being the most concerned users. Similarly, pragmatists could be modelled to realise negative consequences slower (i.e., long delay) and interpret them as somewhat worse, thus being less concerned than fundamentalists. Finally, unconcerned could be the least able to understand what the privacy fuss is all about, thus being the least concerned users. As a result, the inconsistency between privacy concerns and actual behaviour that indicates the privacy paradox would also vary in extent between the three user groups. In addition, not all three user groups would share the same amount of data, thus not all data shared by each user group would be useful for processing (Aggregation and Downstream Uses) by the platform and third parties.

Finally, the methodological approach of using system dynamics could be used for studying the privacy paradox outside the context of social media. For example, the model could be applied to further types of platforms, such as peer-to-peer (P2P) platforms (e.g., Airbnb and Uber), in order to test and expand the privacy paradox study to additional contexts.

8. Conclusions

This article incorporates existing privacy knowledge, including all eight privacy obstacles, into a qualitative system dynamics model and examines the conditions under which the privacy paradox emerges over time in the context of social media. The results show that the eight privacy obstacles prevent adequately accounting for the negative consequences of adopting and using social media by (1) reinforcing gratifications, thus inducing social media adoption and use, while (2) hampering the realisation of (all) negative consequences, thus reducing the motivation for social media discard. Moreover, gratifications kick off early and often seem to dominate even major long-term negative consequences, thereby resulting in users becoming only gradually concerned about privacy, by which time they are usually deeply engaged in the platform to consider discarding, and therefore arriving in a paradoxical situation that seems not viable to escape from (i.e., the boiling frog syndrome). Conversely, major short-term negative consequences are more likely to conflict with gratifications already earlier, thereby resulting in users becoming less engaged, more concerned,

and therefore still able to discard the platform, thus resolving the paradoxical situation. Thereby, the article paves the way towards a more comprehensive *synthetic* privacy paradox explanation that is still missing from current privacy literature [12] and is difficult to be provided using only conventional cross-sectional approaches.

Author Contributions: Conceptualization, E.A., Y.K., S.R. and T.E.; methodology, E.A. and S.R.; validation, E.A., Y.K. and S.R.; formal analysis, E.A., Y.K. and S.R.; writing—original draft preparation, E.A.; writing—review and editing, Y.K. and S.R.; visualization, E.A.; supervision, Y.K. and S.R.; project administration, Y.K. and T.E.; funding acquisition, T.E. All authors have read and agreed to the published version of the manuscript.

Funding: This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 964678.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank Pekka Nikander for his insightful comments.

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

References

1. van Dijck, J. Facebook and the Engineering of Connectivity: A Multi-Layered Approach to Social Media Platforms. *Convergence* **2013**, *19*, 141–155. [CrossRef]
2. van Dijck, J. 'You Have One Identity': Performing the Self on Facebook and LinkedIn. *Media Cult. Soc.* **2013**, *35*, 199–215. [CrossRef]
3. Zuboff, S. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *J. Inf. Technol.* **2015**, *30*, 75–89. [CrossRef]
4. West, S.M. Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Bus. Soc.* **2019**, *58*, 20–41. [CrossRef]
5. Custers, B.; Malgieri, G. Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data. *Comput. Law Secur. Rev.* **2022**, *45*, 105683. [CrossRef]
6. Rughiniș, R.; Rughiniș, C.; Vulpe, S.N.; Rosner, D. From Social Netizens to Data Citizens: Variations of GDPR Awareness in 28 European Countries. *Comput. Law Secur. Rev.* **2021**, *42*, 105585. [CrossRef]
7. Statista. Online Privacy and Data Protection in the European Union (EU), 2016. Available online: https://www.statista.com/study/38093/online-privacy-and-data-protection-in-the-european-union-eu-statista-dossier/ (accessed on 15 February 2023).
8. Statista. Online Privacy in the United States, 2020. Available online: https://www.statista.com/study/17352/online-privacy-statista-dossier/ (accessed on 15 February 2023).
9. Brown, B. *Studying the Internet Experience*; HP Laboratories Technical Report 49; Hewlett-Packard Company: Palo Alto, CA, USA, 2001.
10. Norberg, P.A.; Horne, D.R.; Horne, D.A. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *J. Consum. Aff.* **2007**, *41*, 100–126. [CrossRef]
11. Barth, S.; de Jong, M.D.T. The Privacy Paradox—Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review. *Telemat. Inform.* **2017**, *34*, 1038–1058. [CrossRef]
12. Kokolakis, S. Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. *Comput. Secur.* **2017**, *64*, 122–134. [CrossRef]
13. 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]
14. Lehtiniemi, T.; Kortesniemi, Y. Can the Obstacles to Privacy Self-Management Be Overcome? Exploring the Consent Intermediary Approach. *Big Data Soc.* **2017**, *4*, 1–11. [CrossRef]
15. Sterman, J.D. *Business Dynamics: Systems Thinking and Modeling for a Complex World*; McGraw-Hill: New York, NY, USA, 2000.
16. Goldstein, L. How to Boil a Live Frog. *Analysis* **2000**, *60*, 170–178. [CrossRef]
17. Buzeta, C.; De Pelsmacker, P.; Dens, N. Motivations to Use Different Social Media Types and Their Impact on Consumers' Online Brand-Related Activities (COBRAs). *J. Interact. Mark.* **2020**, *52*, 79–98. [CrossRef]
18. Katz, E.; Haas, H.; Gurevitch, M. On the Use of the Mass Media for Important Things. *Am. Sociol. Rev.* **1973**, *38*, 164–181. [CrossRef]
19. Katz, E.; Blumler, J.G.; Gurevitch, M. Uses and Gratifications Research. *Public Opin. Q.* **1973**, *37*, 509–523. [CrossRef]
20. McQuail, D. *Mass Communication Theory: An Introduction*; SAGE Publications: London, UK, 1987.
21. Muntinga, D.G.; Moorman, M.; Smit, E.G. Introducing COBRAs. *Int. J. Advert.* **2011**, *30*, 13–46. [CrossRef]

22. Mull, I.R.; Lee, S.E. "PIN" Pointing the Motivational Dimensions Behind Pinterest. *Comput. Hum. Behav.* **2014**, *33*, 192–200. [CrossRef]
23. Phua, J.; Jin, S.V.; Kim, J.J. Gratifications of Using Facebook, Twitter, Instagram, or Snapchat to Follow Brands: The Moderating Effect of Social Comparison, Trust, Tie Strength, and Network Homophily on Brand Identification, Brand Engagement, Brand Commitment, and Membership Intention. *Telemat. Inform.* **2017**, *34*, 412–424. [CrossRef]
24. Sheldon, P.; Rauschnabel, P.A.; Antony, M.G.; Car, S. A Cross-Cultural Comparison of Croatian and American Social Network Sites: Exploring Cultural Differences in Motives for Instagram Use. *Comput. Hum. Behav.* **2017**, *75*, 643–651. [CrossRef]
25. Sjöblom, M.; Hamari, J. Why Do People Watch Others Play Video Games? An Empirical Study on the Motivations of Twitch Users. *Comput. Hum. Behav.* **2017**, *75*, 985–996. [CrossRef]
26. Sumter, S.R.; Vandenbosch, L.; Ligtenberg, L. Love Me Tinder: Untangling Emerging Adults' Motivations for Using the Dating Application Tinder. *Telemat. Inform.* **2017**, *34*, 67–78. [CrossRef]
27. Pittman, M.; Reich, B. Social Media and Loneliness: Why an Instagram Picture May Be Worth More Than a Thousand Twitter Words. *Comput. Hum. Behav.* **2016**, *62*, 155–167. [CrossRef]
28. Casale, S.; Fioravanti, G. Why Narcissists Are at Risk for Developing Facebook Addiction: The Need to Be Admired and the Need to Belong. *Addict. Behav.* **2018**, *76*, 312–318. [CrossRef]
29. Sheldon, P.; Bryant, K. Instagram: Motives for Its Use and Relationship to Narcissism and Contextual Age. *Comput. Hum. Behav.* **2016**, *58*, 89–97. [CrossRef]
30. Khan, M.L. Social Media Engagement: What Motivates User Participation and Consumption on YouTube? *Comput. Hum. Behav.* **2017**, *66*, 236–247. [CrossRef]
31. Lin, Y.H.; Hsu, C.L.; Chen, M.F.; Fang, C.H. New Gratifications for Social Word-of-Mouth Spread via Mobile SNSs: Uses and Gratifications Approach with a Perspective of Media Technology. *Telemat. Inform.* **2017**, *34*, 382–397. [CrossRef]
32. Lim, H.; Kumar, A. Variations in Consumers' Use of Brand Online Social Networking: A Uses and Gratifications Approach. *J. Retail. Consum. Serv.* **2019**, *51*, 450–457. [CrossRef]
33. Leung, L. Generational Differences in Content Generation in Social Media: The Roles of the Gratifications Sought and of Narcissism. *Comput. Hum. Behav.* **2013**, *29*, 997–1006. [CrossRef]
34. Chen, C.Y.; Chang, S.L. User-Orientated Perspective of Social Media Used by Campaigns. *Telemat. Inform.* **2017**, *34*, 811–820. [CrossRef]
35. Erz, A.; Marder, B.; Osadchaya, E. Hashtags: Motivational Drivers, Their Use, and Differences Between Influencers and Followers. *Comput. Hum. Behav.* **2018**, *89*, 48–60. [CrossRef]
36. Leiner, D.J.; Kobilke, L.; Rueß, C.; Brosius, H.B. Functional Domains of Social Media Platforms: Structuring the Uses of Facebook to Better Understand Its Gratifications. *Comput. Hum. Behav.* **2018**, *83*, 194–203. [CrossRef]
37. Trepte, S.; Scharkow, M.; Dienlin, T. The Privacy Calculus Contextualized: The Influence of Affordances. *Comput. Hum. Behav.* **2020**, *104*, 106115. [CrossRef]
38. Heravi, A.; Mubarak, S.; Raymond Choo, K.K. Information Privacy in Online Social Networks: Uses and Gratification Perspective. *Comput. Hum. Behav.* **2018**, *84*, 441–459. [CrossRef]
39. Rosenberg, R.S. *The Social Impact of Computers*; Academic Press Inc.: Cambridge, MA, USA, 1992.
40. Holvast, J. Vulnerability and Privacy: Are We on the Way to a Risk-Free Society? *Facing Chall. Risk Vulnerability Inf. Soc.* **1993**, *33*, 267–279.
41. Westin, A.F. *Privacy and Freedom*; Atheneum: Berlin, Germany, 1967.
42. Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*; Brooks/Cole: Monterey, CA, USA, 1975.
43. Altman, I. Privacy Regulation: Culturally Universal or Culturally Specific? *J. Soc. Issues* **1977**, *33*, 66–84. [CrossRef]
44. Petronio, S. *Boundaries of Privacy: Dialectics of Disclosure*; State University of New York Press: Albany, NY, USA, 2002.
45. Westin, A.F. Social and Political Dimensions of Privacy. *J. Soc. Issues* **2003**, *59*, 431–453. [CrossRef]
46. Arzoglou, E.; Kortesniemi, Y.; Ruutu, S.; Elo, T. Privacy Paradox in Social Media: A System Dynamics Analysis. In *Computational Science—ICCS 2022*; Lecture Notes in Computer Science; Groen, D., de Mulatier, C., Paszynski, M., Dongarra, J.J., Sloot, P.M.A., Eds.; Springer: Cham, Switzerland, 2022; Volume 13350, pp. 651–666.
47. Culnan, M.J.; Armstrong, P.K. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organ. Sci.* **1999**, *10*, 104–115. [CrossRef]
48. Solove, D. Privacy Self-Management and the Consent Dilemma. *Harv. Law Rev.* **2013**, *126*, 1880–1903.
49. Tversky, A.; Kahneman, D. Judgment Under Uncertainty: Heuristics and Biases. *Science* **1974**, *185*, 1124–1131. [CrossRef]
50. Acquisti, A.; Grossklags, J. Privacy and Rationality in Individual Decision Making. *IEEE Secur. Priv.* **2005**, *3*, 26–33. [CrossRef]
51. Acquisti, A.; Grossklags, J. What Can Behavioral Economics Teach Us About Privacy? In *Digital Privacy: Theory, Technologies, and Practices*; CRC Press: Boca Raton, FL, USA, 2007; pp. 363–377.
52. Flender, C.; Müller, G. Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited. In *Quantum Interaction—QI 2012*; Lecture Notes in Computer Science; Busemeyer, J.R., Dubois, F., Lambert-Mogiliansky, A., Melucci, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7620, pp. 148–159.
53. Simon, H.A. *Models of Bounded Rationality, Volume 1: Economic Analysis and Public Policy*; MIT Press: Cambridge, MA, USA, 1982.
54. Slovic, P.; Finucane, M.L.; Peters, E.; MacGregor, D.G. The Affect Heuristic. *Eur. J. Oper. Res.* **2007**, *177*, 1333–1352. [CrossRef]

55. Schwarz, N.; Bless, H.; Strack, F.; Klumpp, G.; Rittenauer-Schatka, H.; Simons, A. Ease of Retrieval as Information: Another Look at the Availability Heuristic. *J. Personal. Soc. Psychol.* **1991**, *61*, 195–202. [CrossRef]
56. Plous, S. *The Psychology of Judgment and Decision Making*; McGraw-Hill: New York, NY, USA, 1993.
57. Acquisti, A.; Grossklags, J. Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior. In Proceedings of the 2nd Annual Workshop on Economics and Information Security (WEIS 2003), College Park, MD, USA, 29–30 May 2003.
58. Cho, H.; Lee, J.S.; Chung, S. Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience. *Comput. Hum. Behav.* **2010**, *26*, 987–995. [CrossRef]
59. Moore, D.A.; Healy, P.J. The Trouble with Overconfidence. *Psychol. Rev.* **2008**, *115*, 502–517. [CrossRef]
60. Langer, E.J. The Illusion of Control. *J. Personal. Soc. Psychol.* **1975**, *32*, 311–328. [CrossRef]
61. Sterman, J.D. Misperceptions of Feedback in Dynamic Decision Making. *Organ. Behav. Hum. Decis. Process.* **1989**, *43*, 301–335. [CrossRef]
62. Sterman, J.D. Modeling Managerial Behavior: Misperceptions of Feedback in a Dynamic Decision Making Experiment. *Manag. Sci.* **1989**, *35*, 321–339. [CrossRef]
63. Blank, G.; Bolsover, G.; Dubois, E. A New Privacy Paradox: Young People and Privacy on Social Network Sites. In Proceedings of the 109th Annual Meeting of the American Sociological Association (ASA Annual Meeting 2014), San Francisco, CA, USA, 16–19 August 2014.
64. Hull, G. Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data. *Ethics Inf. Technol.* **2015**, *17*, 89–101. [CrossRef]
65. Nemec Zlatolas, L.; Welzer, T.; Heričko, M.; Hölbl, M. Privacy Antecedents for SNS Self-Disclosure: The Case of Facebook. *Comput. Hum. Behav.* **2015**, *45*, 158–167. [CrossRef]
66. 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]
67. Happ, C.; Melzer, A.; Steffgen, G. Trick with Treat—Reciprocity Increases the Willingness to Communicate Personal Data. *Comput. Hum. Behav.* **2016**, *61*, 372–377. [CrossRef]
68. Tufekci, Z. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bull. Sci. Technol. Soc.* **2008**, *28*, 20–36. [CrossRef]
69. Taddicken, M. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *J. Comput.-Mediat. Commun.* **2014**, *19*, 248–273. [CrossRef]
70. Dienlin, T.; Trepte, S. Is the Privacy Paradox a Relic of the Past? An In-Depth Analysis of Privacy Attitudes and Privacy Behaviors. *Eur. J. Soc. Psychol.* **2015**, *45*, 285–297. [CrossRef]
71. Boyd, D.; Hargittai, E. Facebook Privacy Settings: Who Cares? *First Monday* **2010**, *15*. [CrossRef]
72. Young, A.L.; Quan-Haase, A. Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited. *Inform. Commun. Soc.* **2013**, *16*, 479–500. [CrossRef]
73. 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]
74. Custers, B. Click Here to Consent Forever: Expiry Dates for Informed Consent. *Big Data Soc.* **2016**, *3*, 1–6. [CrossRef]
75. Taylor, T.; Ford, D.N. Tipping Point Failure and Robustness in Single Development Projects. *Syst. Dyn. Rev.* **2006**, *22*, 51–71. [CrossRef]
76. Repenning, N.P. Understanding Fire Fighting in New Product Development. *J. Prod. Innov. Manag.* **2001**, *18*, 285–300. [CrossRef]
77. Rahmandad, H.; Repenning, N.P. Capability Erosion Dynamics. *Strateg. Manag. J.* **2016**, *37*, 649–672. [CrossRef]
78. Rudolph, J.W.; Repenning, N.P. Disaster Dynamics: Understanding the Role of Quantity in Organizational Collapse. *Adm. Sci. Q.* **2002**, *47*, 1–30. [CrossRef]
79. Shin, M.; Lee, H.S.; Park, M.; Moon, M.; Han, S. A System Dynamics Approach for Modeling Construction Workers' Safety Attitudes and Behaviors. *Accid. Anal. Prev.* **2014**, *68*, 95–105. [CrossRef] [PubMed]
80. Ruutu, S.; Casey, T.; Kotovirta, V. Development and Competition of Digital Service Platforms: A System Dynamics Approach. *Technol. Forecast. Soc. Chang.* **2017**, *117*, 119–130. [CrossRef]
81. Rahmandad, H.; Repenning, N.P.; Sterman, J.D. Effects of Feedback Delay on Learning. *Syst. Dyn. Rev.* **2009**, *25*, 309–338. [CrossRef]
82. Rogers, E.M. *Diffusion of Innovations*; Free Press: New York, NY, USA, 2003.
83. Bass, F.M. A New Product Growth for Model Consumer Durables. *Manag. Sci.* **1969**, *15*, 215–227. [CrossRef]
84. Katz, M.L.; Shapiro, C. Technology Adoption in the Presence of Network Externalities. *J. Political Econ.* **1986**, *94*, 822–841. [CrossRef]
85. Acquisti, A.; Brandimarte, L.; Loewenstein, G. Privacy and Human Behavior in the Age of Information. *Science* **2015**, *347*, 509–514. [CrossRef]
86. Evans, D.S. *Platform Economics: Essays on Multi-Sided Businesses*; Competition Policy International: Boston, MA, USA, 2011.
87. Evans, D.S.; Schmalensee, R. *Matchmakers: The New Economics of Multisided Platforms*; Harvard Business Review Press: Boston, MA, USA, 2016.

88. van Dijck, J. Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology. *Surveill. Soc.* **2014**, *12*, 197–208. [CrossRef]
89. Press Association. Hacker Advertises Details of 117 Million LinkedIn Users on Darknet. *The Guardian*. 2016. Available online: https://www.theguardian.com/technology/2016/may/18/hacker-advertises-details-of-117-million-linkedin-users-on-darknet/ (accessed on 15 February 2023).
90. Bernal, N. Google Accused of Secretly Feeding Personal Data to Advertisers. *The Telegraph*. 2019. Available online: https://www.telegraph.co.uk/technology/2019/09/04/google-accused-secretly-feeding-personal-data-advertisers/ (accessed on 15 February 2023).
91. Wong, J.C. Facebook Confirms 419m Phone Numbers Exposed in Latest Privacy Lapse. *The Guardian*. 2019. Available online: https://www.theguardian.com/technology/2019/sep/04/facebook-users-phone-numbers-privacy-lapse/ (accessed on 15 February 2023).
92. Dodds, L. Phone Numbers of 11.5m Britons Leaked Online in Facebook Breach That Also Exposed Mark Zuckerberg. *The Telegraph*. 2021. Available online: https://www.telegraph.co.uk/technology/2021/04/05/phone-numbers-115m-brits-leaked-online-facebook-breach-also/ (accessed on 15 February 2023).
93. Meaker, M. Telegram, Signal, WhatsApp and Facebook: Which Is Better? *The Telegraph*. 2021. Available online: https://www.telegraph.co.uk/technology/0/telegram-signal-whatsapp-facebook-better/ (accessed on 15 February 2023).
94. Meyers, E.M.; Erickson, I.; Small, R.V. Digital Literacy and Informal Learning Environments: An Introduction. *Learn. Media Technol.* **2013**, *38*, 355–367. [CrossRef]
95. Debatin, B. Ethics, Privacy, and Self-Restraint in Social Networking. In *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 47–60.
96. Trepte, S.; Teutsch, D.; Masur, P.K.; Eicher, C.; Fischer, M.; Hennhöfer, A.; Lind, F. Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In *Reforming European Data Protection Law*; Law, Governance and Technology Series; Springer: Dordrecht, Germany, 2015; pp. 333–365.
97. Frederick, S.; Loewenstein, G.; O'Donoghue, T. Time Discounting and Time Preference: A Critical Review. *J. Econ. Lit.* **2002**, *40*, 351–401. [CrossRef]
98. Downs, A. An Economic Theory of Political Action in a Democracy. *J. Political Econ.* **1957**, *65*, 135–150. [CrossRef]
99. Hargittai, E.; Marwick, A. "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *Int. J. Commun.* **2016**, *10*, 3737–3757.
100. Baruh, L.; Secinti, E.; Cemalcilar, Z. Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *J. Commun.* **2017**, *67*, 26–53. [CrossRef]
101. Brough, A.R.; Martin, K.D. Critical Roles of Knowledge and Motivation in Privacy Research. *Curr. Opin. Psychol.* **2020**, *31*, 11–15. [CrossRef]
102. Brandimarte, L.; Acquisti, A.; Loewenstein, G. Misplaced Confidences: Privacy and the Control Paradox. *Soc. Psychol. Personal. Sci.* **2013**, *4*, 340–347. [CrossRef]
103. Boerman, S.C.; Kruikemeier, S.; Zuiderveen Borgesius, F.J. Exploring Motivations for Online Privacy Protection Behavior: Insights from Panel Data. *Commun. Res.* **2021**, *48*, 953–977. [CrossRef]
104. Bartsch, M.; Dienlin, T. Control Your Facebook: An Analysis of Online Privacy Literacy. *Comput. Hum. Behav.* **2016**, *56*, 147–154. [CrossRef]
105. Agarwal, R.; Karahanna, E. Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage. *MIS Q.* **2000**, *24*, 665–694. [CrossRef]
106. Alashoor, T.; Baskerville, R. The Privacy Paradox: The Role of Cognitive Absorption in the Social Networking Activity. In Proceedings of the 36th International Conference on Information Systems (ICIS 2015), Fort Worth, TX, USA, 13–16 December 2015.
107. Trang, S.; Weiger, W.H. The Perils of Gamification: Does Engaging with Gamified Services Increase Users' Willingness to Disclose Personal Information? *Comput. Hum. Behav.* **2021**, *116*, 106644. [CrossRef]
108. Wong, J.C. Facebook Says Nearly 50m Users Compromised in Huge Security Breach. *The Guardian*. 2018. Available online: https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach/ (accessed on 15 February 2023).
109. Statista. Facebook's Daily Active User (DAU) Figures in Europe from 4th Quarter 2012 to 1st Quarter 2020. Available online: https://www.statista.com/statistics/745383/facebook-europe-dau-by-quarter/ (accessed on 15 February 2023).
110. Statista. Facebook's Monthly Active Users (MAU) in Europe from 4th Quarter 2012 to 1st Quarter 2021. Available online: https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/ (accessed on 15 February 2023).
111. Statista. Number of Monthly Active WhatsApp Users Worldwide from April 2013 to March 2020. Available online: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/ (accessed on 15 February 2023).
112. Statista. Number of Monthly Active Instagram Users from January 2013 to June 2018. Available online: https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/ (accessed on 15 February 2023).
113. Halliday, J. Google Agrees to Privacy Reviews to Settle Buzz Complaint. *The Guardian*. 2011. Available online: http://www.theguardian.com/technology/2011/mar/30/google-privacy-reviews-buzz-ftc/ (accessed on 15 February 2023).
114. Hern, A. Closure of Google+: Everything You Need to Know. *The Guardian*. 2019. Available online: http://www.theguardian.com/technology/2019/feb/01/closure-google-plus-everything-you-need-to-know/ (accessed on 15 February 2023).

115. Crain, M. The Limits of Transparency: Data Brokers and Commodification. *New Media Soc.* **2018**, *20*, 88–104. [CrossRef]
116. Crutchfield, R.S. Conformity and Character. *Am. Psychol.* **1955**, *10*, 191–198. [CrossRef]
117. Tönnies, F. *Community and Society*; Dover Publications: New York, NY, USA, 2003.
118. Seligman, M.E.P. Learned Helplessness. *Annu. Rev. Med.* **1972**, *23*, 407–412. [CrossRef] [PubMed]
119. Choi, H.; Park, J.; Jung, Y. The Role of Privacy Fatigue in Online Privacy Behavior. *Comput. Hum. Behav.* **2018**, *81*, 42–51. [CrossRef]
120. Kortesniemi, Y.; Kremer, J. Recommendations and Automation in the Consenting Process: Designing GDPR Compliant Consents. In Proceedings of the Legal Design as Academic Discipline: Foundations, Methodology, Applications, Groningen, The Netherlands, 12 December 2018.
121. Kortesniemi, Y.; Lappalainen, T.; Salka, F. User Attitudes Towards Consent Intermediaries. In Proceedings of the Legal Design as Academic Discipline: Foundations, Methodology, Applications, Groningen, The Netherlands, 12 December 2018.