Privacy paradox in social media: A system dynamics analysis

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

Aalto University
Department of Communications and Networking
{ektor.arzoglou,yki.kortesniemi,sampsa.ruutu,tommi.elo}@aalto.fi

Abstract. The term 'privacy paradox' refers to the apparent inconsistency between people's concerns about their privacy and their actual privacy behaviour. Although several possible explanations for this phenomenon have been provided so far, these assume that (1) all people share the same privacy concerns and (2) a snapshot at a given point in time is enough to explain the phenomenon. To overcome these limitations, this article presents a system dynamics simulation model that considers the diversity of privacy concerns during the process of social media adoption and identifies the types of situations in which the privacy paradox emerges. The results show that (1) the least concerned minority can induce the more concerned majority to adopt social media and (2) even the most concerned minority can be hindered by the less concerned majority from discarding social media. Both (1) and (2) are types of situations that reflect the privacy paradox.

Keywords: Digital platforms · Privacy · Privacy paradox · Social media · System dynamics

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 [8]. Users actively construct their online identities, engage in active data sharing, and therefore satisfy various personal and professional needs. As a result, the influence exerted by current users on potential users to also adopt social media is reinforced and, as it evolves into a *social norm*, it becomes harder to resist regardless of privacy preferences and concerns [1]. At the same time, surveys show that people who use social media every day are highly concerned about the data collected about them on the Internet [12]. This inconsistency of privacy concerns and actual behaviour is often referred to as the *privacy paradox* [4, 9].

Over the last couple of decades, privacy researchers have provided several possible explanations for the privacy paradox, with studies assuming that (1) all people share the same privacy concerns [9] and (2) a snapshot at a given point in time is enough to explain the phenomenon. However, privacy concerns are not

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

of the same degree for all people [15]. Moreover, the cross-sectional approaches, such as surveys and experiments, used in previous privacy paradox studies do not explain the changes in privacy concerns over time [9]. These limitations can be addressed with a process theory, hence motivating the development of a simulation model using *system dynamics* [13] in this article.

The research question guiding this article is: *In what types of situations can a social norm outweigh privacy concerns, thus resulting in social media adoption, and how does this help understand the privacy paradox?* The results of the developed system dynamics simulation model show that (1) the least concerned minority can induce the more concerned majority to adopt social media and (2) even the most concerned minority can be hindered by the less concerned majority from discarding social media. Both (1) and (2) are types of situations that reflect the privacy paradox. 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 reviews literature on informational privacy and privacy paradox. Section 3 describes the applicability of the methodology used, namely system dynamics modelling, to the privacy paradox. Section 4 presents the model of the social media platform. The simulation results are discussed in Section 5. Finally, Section 6 concludes the article.

2 Theoretical background

The concept of privacy has three main aspects: (1) *territorial privacy*, protecting the close physical area surrounding a person, (2) *privacy of the person*, protecting a person against undue interference, and (3) *informational privacy*, controlling whether and how personal data can be gathered, stored, processed, or selectively disseminated [9, 10]. This article focuses exclusively on the third aspect.

2.1 Informational privacy

One of the most influential privacy theories is that developed by Alan Westin, who 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" [14]. In addition, Westin discusses privacy as a *dynamic* process (i.e. over time) of interpersonal boundary control and argues that 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 [15].

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

Westin's theory focuses on informational privacy and, since the focus of this article is exclusively on informational privacy as well, Westin's privacy segmentation acts as driver for the model development.

2.2 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 [4,9]. 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 [9]. The explanations are summarised in Table 1.

Table 1. Privacy paradox explanations

Explanation	Description
Privacy calculus	People perform a perfectly informed and rational cost-benefit analysis and decide to share their data only when benefits outweigh costs. However, they might still express concerns about the privacy of their shared data, resulting in the inconsistency between expressed privacy concerns (or attitude) and actual behaviour.
Incomplete information, bounded rationality, and decision biases	People use heuristics, which compensate for limitations in information, time, and cognitive capabilities, in order to make decisions. However, these heuristics often result in unexpected outcomes.
Social influence	People's behaviour is influenced by social factors and therefore might not match their unbiased attitude.

3 A system dynamics model of the privacy paradox

System dynamics is a methodology that uses feedback loops, accumulations, and time delays to understand the *behaviour of complex systems over time* [13]. One of the primary strengths of system dynamics is that it allows for the inclusion of both social and technical elements into the same model and therefore the study of complex sociotechnical systems, such as social media.

Over the last decade, researchers have started to conceptualise digital platforms and multi-sided markets as dynamic systems and use system dynamics to study related phenomena, such as platform adoption, over time [5,11]. However, these studies neglect the fact that privacy concerns are a significant factor in

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

the adoption of online services, such as digital platforms [6], and therefore the concept of privacy concerns is missing from existing platform adoption models. To overcome this limitation, this article presents a system dynamics simulation model that considers the diversity of privacy concerns during the process of social media adoption and identifies the types of situations in which the privacy paradox emerges.

In system dynamics, the model development is preceded by (1) *reference modes*, which are graphs illustrating the problem (e.g. the privacy paradox) as a pattern of behaviour over time, and (2) a *dynamic hypothesis*, which aims to explain the problematic behaviour shown in the reference modes in terms of the underlying *feedback and stock-flow structure* (see Section 4) of the system [13].

3.1 Problem articulation

In order to illustrate the privacy paradox in the context of social media, this article uses four reference modes that are most relevant to platform adoption: (1) there is a growth in platform adoption that ultimately stabilises (i.e. S-shaped growth) (e.g. a social media platform can be steadily adopted by highly concerned users, who are influenced by less concerned users), (2) the S-shaped growth of platform adoption is followed by a minor decline, which ultimately stabilises (e.g. a social media platform can maintain a large fraction of highly concerned users, who are hindered by less concerned users from discarding), (3) an initial period of growth in platform adoption is followed by a decline, but platform adoption subsequently overtakes this decline and continues to grow until it ultimately stabilises (e.g. a social media platform can experience only a transient loss of highly concerned users, who discard but are eventually influenced by less concerned users to re-adopt), and (4) an initial period of growth in platform adoption is followed by a collapse (i.e. overshoot and collapse) (e.g. a social media platform can be discarded by highly concerned users, who also influence less concerned users). Reference modes (1)-(3) illustrate situations in which privacy concerns are inconsistent with platform adoption, thus reflecting the privacy paradox, whereas in (4) privacy concerns are consistent with platform discard, thus not reflecting the privacy paradox.

The purpose of the model is to explain the types of situations in which a social norm can outweigh privacy concerns using these four modes of dynamic behaviour. As these dynamic behaviours can occur in different settings, the model was built as a generic representation of social media without focusing on any specific platform. Finally, the time horizon of the model is in the order of multiple years, so that the entire platform adoption phase is included in the simulation results.

3.2 Dynamic hypothesis

The dynamic hypothesis guiding the model development is that an extended feedback structure of the Bass model of *innovation diffusion*, which describes the adoption of new products or services (over time) [3], can produce the four

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

modes of dynamic behaviour. As such, platform adoption can be influenced by different factors, such as privacy concerns, that have an effect on the feedback loops of the model.

The model includes a social media platform of potential and current users that is modelled *endogenously*. That is, every platform variable is affected by one or more other platform variables. Conversely, since privacy concerns can be described as a merely negative concept not bound to any specific context [7, 9], they are modelled *exogenously*. That is, privacy concerns affect but are not affected by the platform.

4 Model development

In system dynamics, (1) *stocks*, represented by rectangles, are accumulations of either matter or information, (2) *flows*, represented by pipes and valves, regulate the rate of change of the stocks, and (3) *auxiliaries*, represented by intermediate variables between stocks and flows, clarify the sequence of events that cause the flows to change the stocks.

Variables at the tail of the causal links are independent, indicating a cause, while variables at the head of the causal links are dependent, indicating an effect. All causal links indicate that a change in the independent variable causes the dependent variable to change in the *same* direction, except for these labelled with a minus sign (-) that indicate a change in the *opposite* direction.

Finally, *feedback* is the process whereby an initial cause gradually spreads through a chain of causal links to ultimately re-affect itself, thereby forming a loop that can be either *reinforcing* (R) (i.e. amplifying causal changes) or *balancing* (B) (i.e. counteracting and opposing causal changes). In this case, variables constituting feedback loops are at the same time both causes and effects.

4.1 Model structure

The social media platform is modelled by extending the Bass model of innovation diffusion, which considers adoption through exogenous efforts, such as advertising, and adoption through word-of-mouth [3] (Figure 1). In addition, the model utilises several equations from Ruutu et al. [11].

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 (R1: "WoM"). As the stock of users grows, platform value increases, and the norm related to platform adoption becomes stronger and consequently harder to deviate from. As a result, more potential users conform and adopt the platform (R2: "Social Norm"). 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, B2: "Market Saturation"). Finally, current users may decide to discard the platform and re-enter the stock of potential users (since they may be persuaded to adopt

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

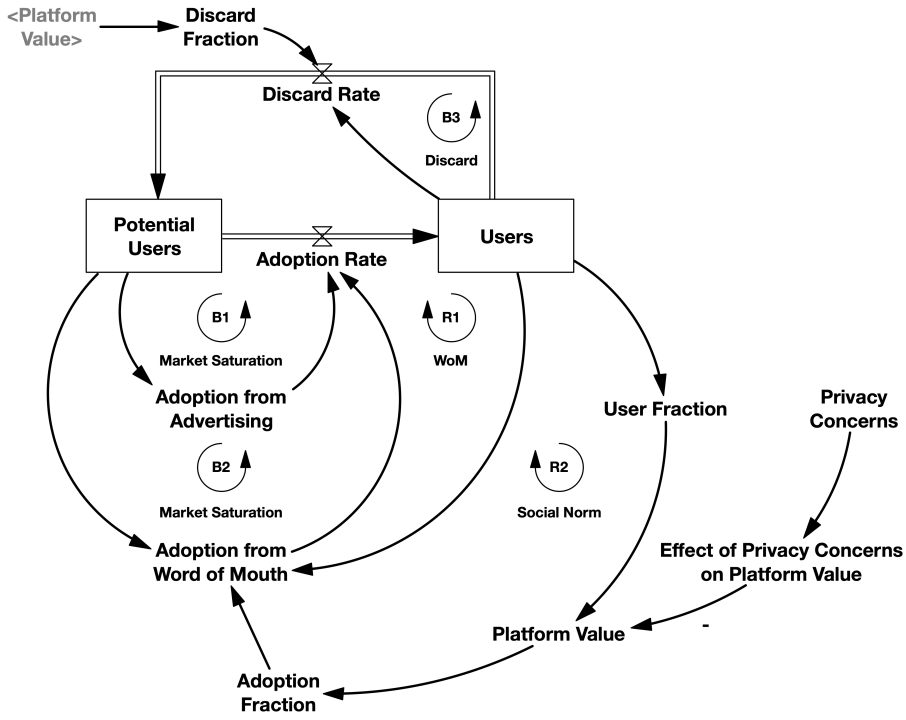

Fig. 1. Social media adoption affected by social norm and privacy concerns

again in the future). In this case, the discard rate depends on the number of current users and the decrease, caused by privacy concerns, in platform value (B3: "Discard").

The behaviour of potential and current users is modelled using rules of bounded rationality, which depend on the information available to users at a given point in time. In other words, potential and current users are not assumed to have perfect foresight of how platform adoption will progress, and they make their decisions regarding platform adoption and discard based on their perception of platform value to them.

4.2 Model parameters

The total population (N) considered in the model is 1000 users, divided into 550 Pragmatists, 250 Fundamentalists, and 200 Unconcerned as per Westin's first privacy segmentation [15]. The degree of privacy concerns for Pragmatists is modelled with parameter P^*, and the additional degree of privacy concerns for Fundamentalists compared to Pragmatists is modelled with parameter F^*, which is a multiplier of P^*. Finally, parameter U^* determines the degree of privacy concerns for Unconcerned. This can range from the extreme condition

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

of zero ($U^* = 1$) to matching the degree of privacy concerns for Pragmatists ($U^* = 0$).

Furthermore, the time at which privacy concerns start is modelled with parameter T^0PC, and the initial value of privacy concerns is modelled with parameter $PC(0)$. The effect of privacy concerns on platform value is modelled using exponential smoothing. Here, parameter τPC is used to determine the erosion of privacy concerns. This essentially indicates the time for users to develop feelings of exhaustion, resignation, and even cynicism towards privacy (i.e. privacy fatigue) [6]. As such, privacy concerns are assumed to be boundedly rational.

In addition to the parameters determining privacy concerns, the model includes eight further parameters that have an effect on platform adoption. First, an external advertising effort (a), starting at time T^0 and ending at time T, is initially required to bring the first users in the platform. Thereafter, platform adoption continues only with word-of-mouth, which depends on the contact rate (c) between potential and current users. Conversely, platform discard depends on parameter τ, which is used to determine the time for users to process the decrease, caused by privacy concerns, in platform value and react by discarding the platform. Moreover, the reference value of platform competitors is modelled with parameter V^*, and the reference user fraction is modelled with parameter uf^*. High values of V^* imply that users receive high value from competitive platforms, and high values of uf^* imply that more users are needed in order to obtain the same level of benefits. Therefore, high values of these two parameters are making platform adoption harder. Finally, the equation of platform value contains an exponent (γ) determining the strength of social norm. High values of γ imply that platform value is strongly dependent on the number of current users. Hence, in the beginning, when there is a lack of users, high values of γ make platform adoption harder. The model equations and parameter values are listed in the Appendix.

4.3 Model testing and validation

The model was built using Vensim DSS for Mac Version 9.0.0 (Double Precision), and the simulation experiments were performed using time step 0.0625 and Euler numerical integration. Several validation tests have been successfully passed to gradually build confidence in the soundness and usefulness of the model. The validation tests assess the validity of the model structure with respect to the purpose presented in Section 3 and are grouped into *direct structure tests*, which do not involve simulation experiments, and *structure-oriented behaviour tests*, in which simulation experiments are used [2]. The results are presented in Table 2.

5 Simulation results

Using the model, it is possible to simulate the four modes of dynamic behaviour presented in Section 3.1 and therefore identify the types of situations in which the privacy paradox emerges.

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

Table 2. Validation tests applied to the model

Test	Result
Direct structure tests	
Structure confirmation	The feedback structures of the model have been formulated and extended based on the Bass model of innovation diffusion [3].
Parameter confirmation	All parameters in the model have clear and meaningful counterparts in the real world. In addition, all parameters were set to limited ranges with minimum and maximum values. Since the model was built as a generic representation of social media, the exact parameter values are not significant, and the parameters have not been estimated based on any specific platform.
Direct extreme condition	The model includes formulations to ensure that stock variables remain valid at all times. For example, the sum of potential and current users stays constant to ensure that conservation laws are met, and the rate of adoption is adjusted with a conditional function (i.e. min) to ensure that the stocks of potential and current users stay non-negative.
Dimensional consistency	The units of all variables and parameters have been specified, and the model passes Vensim's dimensional consistency test.
Structure-oriented behaviour tests	
Indirect extreme condition	The model behaves as expected when individual variables are subjected to extreme conditions. For example, setting the number of users to zero results in zero platform value.
Behaviour sensitivity	The model behaves plausibly when individual parameters are set to the limits of their meaningful ranges of variation as well as when several parameters are varied simultaneously in a Monte Carlo experiment (see Section 5.5).

5.1 Simulation experiment 1

For the first simulation experiment (Figure 2), the degree of privacy concerns is the same for Pragmatists and Fundamentalists ($P^* = 0.5$, $F^* = 1$), on the assumption that the two user groups share the same privacy preferences. In addition, a zero degree of privacy concerns is considered for Unconcerned ($U^* = 1$), assuming that this user group sees no need for privacy.

Initially, platform adoption takes place through advertising (B1) and word-of-mouth (B2, R1) until $Time = 4$. At this point, advertising efforts (B1) end, and platform adoption continues only with word-of-mouth (B2, R1). Moreover, privacy concerns start for Pragmatists and Fundamentalists ($T^0PC = 4$). In the beginning, the effect of privacy concerns on platform value outweighs social norm (R2), causing the number of these two user groups to decline. At the same time, the number of Unconcerned continues to grow, since there is no effect of

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

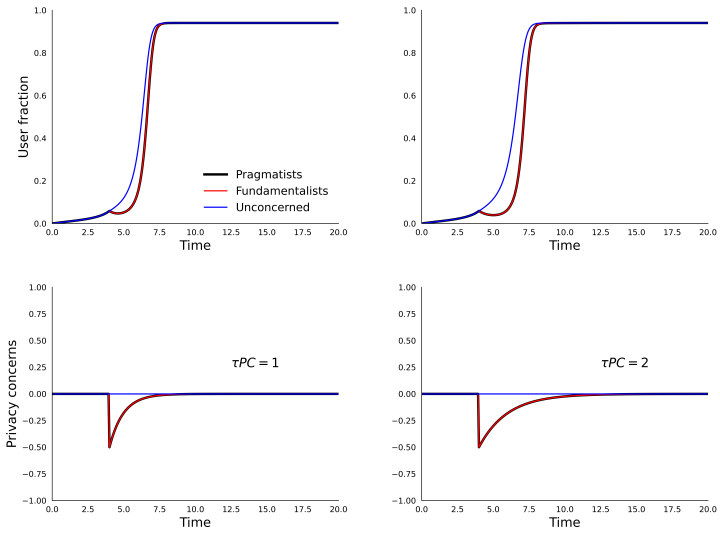

Fig. 2. The social norm created by Unconcerned results in platform adoption also for Pragmatists and Fundamentalists, although privacy concerns of the last two user groups are not eliminated.

privacy concerns to decrease platform value for this user group. In other words, during this phase, discards (B3) dominate adoptions (B2, R1) for Pragmatists and Fundamentalists, while adoptions (B2, R1) continue to dominate discards (B3) for Unconcerned. However, as privacy concerns of Pragmatists and Fundamentalists erode, the effect of privacy concerns on platform value is also falling back. Therefore, as the number of Unconcerned grows, social norm (R2) outweighs privacy concerns of Pragmatists and Fundamentalists, hence recovering platform value for the last two user groups as well. As a result, adoptions (B2, R1) dominate discards (B3) once more for Pragmatists and Fundamentalists, allowing the number of these two user groups to grow again ($Time = 5$). Thus, on one hand, if privacy concerns erode faster ($\tau PC = 1$, left side of Figure 2), platform adoption is easier. On the other hand, if privacy concerns erode slower ($\tau PC = 2$, right side of Figure 2), platform adoption becomes harder. In other words, the slower the erosion of privacy concerns, the longer it takes for social norm to outweigh privacy concerns and therefore the longer the delay in platform adoption.

Both runs of the first simulation experiment illustrate an example of the so called *minority rule*, where the smallest user group of Unconcerned influences the larger user groups of Pragmatists and Fundamentalists. As a result, although privacy concerns of Pragmatists and Fundamentalists are not eliminated, the two user groups eventually adopt the platform, hence resulting in the privacy paradox.

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

5.2 Simulation experiment 2

For the second simulation experiment (Figure 3), the degree of privacy concerns for Fundamentalists is double compared to Pragmatists ($P^* = 0.5$, $F^* = 2$), on the assumption that privacy preferences of Fundamentalists are somewhat stronger. In addition, the degree of privacy concerns for Unconcerned is one-fifth compared to Pragmatists ($U^* = 0.8$), assuming that Unconcerned have significantly less need for privacy than Pragmatists and Fundamentalists. Finally, privacy concerns of Fundamentalists do not erode, on the assumption that this user group is less likely to feel privacy fatigued over time.

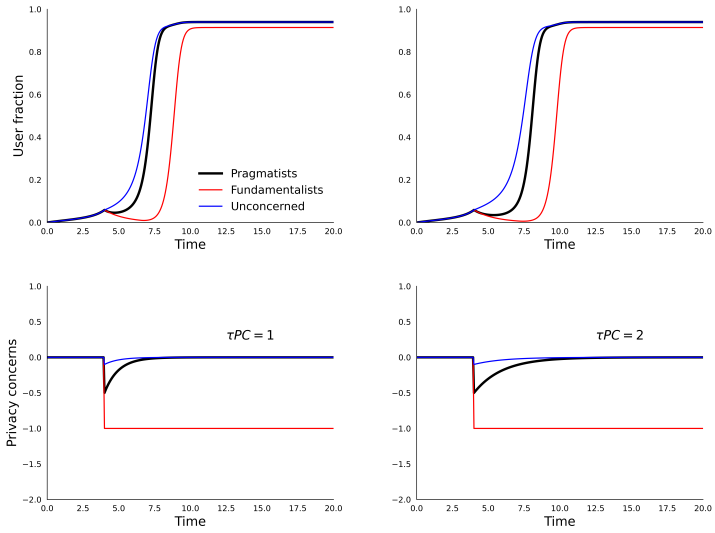

Fig. 3. The social norm created by Pragmatists and Unconcerned results in platform adoption also for Fundamentalists, although privacy concerns of the last user group remain constant.

As before, advertising efforts (B1) end at $Time = 4$, and platform adoption continues only with word-of-mouth (B2, R1). In addition, privacy concerns start for all three user groups ($T^0PC = 4$). At this point, the number of Unconcerned continues to grow as in the previous simulation experiment. The reason is that privacy concerns of this user group are low and have a trivial effect on platform value. At the same time, the number of Pragmatists and Fundamentalists is again starting to decline. However, privacy concerns of Pragmatists erode and are eventually outweighed by social norm (R2), which recovers platform value for this user group, and therefore the number of Pragmatists is once more starting to grow ($Time = 5$). On the other hand, the number of Fundamentalists continues to decline, since privacy concerns of this user group remain constant. Nevertheless, as the number of Pragmatists and Unconcerned grows, social norm (R2)

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

outweighs privacy concerns of Fundamentalists too, hence recovering platform value for the last user group as well. As a result, the number of Fundamentalists starts to grow again ($Time = 7$), although privacy concerns of this user group do not erode. Thus, as before, the faster the erosion of privacy concerns ($\tau PC = 1$, left side of Figure 3), the shorter the delay in platform adoption. Conversely, the slower the erosion of privacy concerns ($\tau PC = 2$, right side of Figure 3), the longer the delay in platform adoption and therefore the more likely the platform adoption is to collapse.

Both runs of the second simulation experiment illustrate once more the minority rule, since the smallest user group of Unconcerned is initially influencing the largest user group of Pragmatists, before both eventually influence the user group of Fundamentalists. As a result, the privacy paradox for Pragmatists is similar to the previous simulation experiment. In addition, although privacy concerns of Fundamentalists remain constant, this user group eventually adopts the platform too, thus exhibiting a more severe privacy paradox.

5.3 Simulation experiment 3

For the third simulation experiment (Figure 4), the degree of privacy concerns is the same for Pragmatists and Fundamentalists ($P^* = 0.5$, $F^* = 1$), on the assumption that the two user groups share the same privacy preferences. In addition, the degree of privacy concerns for Unconcerned is half compared to the first two user groups $U^* = 0.5$), assuming that Unconcerned have somewhat less need for privacy than Pragmatists and Fundamentalists. Finally, privacy concerns erode slower for all three user groups ($\tau PC = 5$), on the assumption that users are less willing to give up their privacy. As a result, platform adoption becomes dependent more on the strength of social norm and less on the erosion of privacy concerns.

Once more, platform adoption takes place through advertising (B1) and word-of-mouth (B2, R1) until $Time = 4$. This is when advertising efforts (B1) end, and platform adoption continues only with word-of-mouth (B2, R1). Here, if the start time of privacy concerns is the same with the previous two simulation experiments ($T^0PC = 4$, left side of Figure 4), the platform's installed user base is small and social norm (R2) weak relative to privacy concerns. Hence, discards (B3) dominate adoptions (B2, R1), causing the stock of users to deplete. In other words, the platform is not able to gather critical mass sufficient to recover platform value from the effect of privacy concerns. Conversely, if privacy concerns start later ($T^0PC = 5$, right side of Figure 4), the user stock is large and social norm (R2) strong relative to privacy concerns. Hence, adoptions (B2, R1) continue to dominate discards (B3), allowing the number of users to grow. In this case, the platform has enough time to gather critical mass sufficient to render platform value nearly unaffected by privacy concerns.

In the first run of the third simulation experiment, no privacy paradox emerges, since privacy concerns are consistent with platform adoption for all three user groups. That is, platform adoption increases when no privacy concerns exist, decreases when privacy concerns start, and collapses while privacy

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

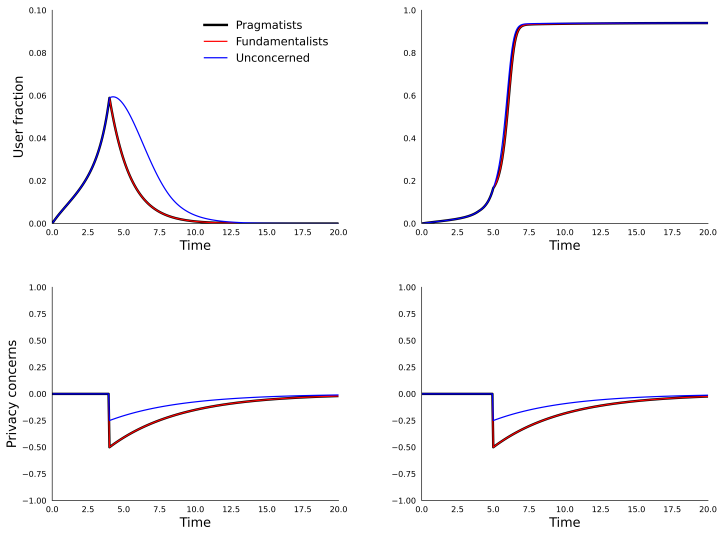

Fig. 4. Weak social norm results in platform adoption collapse because of privacy concerns, whereas strong social norm renders platform adoption nearly unaffected by privacy concerns.

concerns are not eliminated. In the second run, privacy concerns of Pragmatists and Fundamentalists have nearly zero effect on platform adoption of these two user groups, hence resulting in the privacy paradox. In addition, Unconcerned start to exhibit also some extent of the privacy paradox, since this user group is somewhat more concerned here compared to the previous two simulation experiments.

5.4 Simulation experiment 4

For the fourth simulation experiment (Figure 5), the degree of privacy concerns for Fundamentalists is triple compared to Pragmatists ($P^* = 0.5$, $F^* = 3$), on the assumption that privacy preferences of Fundamentalists are significantly stronger. In addition, the degree of privacy concerns for Unconcerned is half compared to Pragmatists $U^* = 0.5$), assuming that Unconcerned have somewhat less need for privacy than Pragmatists and significantly less need for privacy than Fundamentalists. Finally, erosion of privacy concerns applies only to Pragmatists and Unconcerned ($\tau PC = 5$), once more on the assumption that Fundamentalists are less likely to feel privacy fatigued over time.

Here, if the start time of privacy concerns is only one year later compared to the first two simulation experiments ($T^0 PC = 5$, left side of Figure 5), social norm (R2) outweighs privacy concerns of Pragmatists and Unconcerned but is outweighed by privacy concerns of Fundamentalists, thus preserving platform value and adoption only for the first two user groups. By contrast, the number

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

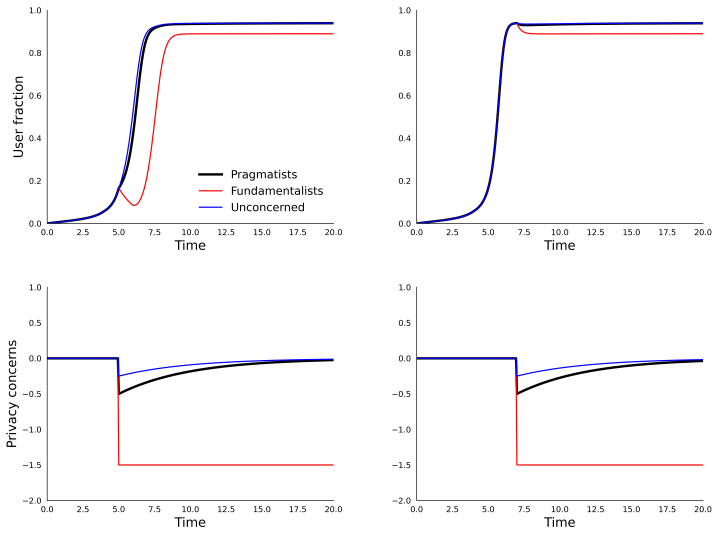

Fig. 5. The social norm created by Pragmatists and Unconcerned results in platform adoption also for a large fraction of Fundamentalists, although privacy concerns of the last user group remain constant.

of Fundamentalists is starting to decline. However, as the number of Pragmatists and Unconcerned grows, social norm (R2) outweighs privacy concerns of Fundamentalists too, hence recovering platform value for the last user group as well. As a result, the number of Fundamentalists starts to grow again ($Time = 6$), although privacy concerns of this user group do not erode. Similarly, if privacy concerns start even later ($T^0PC = 7$, right side of Figure 5), they are once more initially causing the number of Fundamentalists to decline ($Time = 7$), despite the fact that the platform has enough time to gather critical mass. However, social norm (R2) is strong to eventually counterbalance privacy concerns of Fundamentalists, who are therefore hindered from discarding, hence allowing for a large fraction of this user group to remain in the platform ($Time = 8$).

In both runs of the fourth simulation experiment, the privacy paradox for Pragmatists and Unconcerned is similar to the previous simulation experiment. In addition, although privacy concerns of Fundamentalists remain constant, a large fraction of this user group eventually adopts the platform too, thus exhibiting a more severe privacy paradox.

5.5 Sensitivity analysis

The parameters determining the degree (P^*, F^*, and U^*), erosion (τPC), and start time (T^0PC) of privacy concerns are the key factors for the privacy paradox. Low values of τPC and privacy concerns allow for an easier platform adoption, whereas high values of τPC and privacy concerns make platform adoption

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

harder. In other words, higher and more persistent privacy concerns prevent the reinforcement of social norm, hence causing a longer delay in platform adoption and possibly a platform adoption collapse. In this case, the longer the delay in platform adoption, the more likely the platform adoption is to collapse and therefore the less likely the privacy paradox is to emerge. On the other hand, lower and less persistent privacy concerns are more easily outweighed by social norm, hence allowing platform adoption to continue with a shorter delay and resulting in the privacy paradox.

Moreover, low values of T^0PC may cause either a platform adoption collapse, in case of high privacy concerns, or a delay in platform adoption, in case of low privacy concerns. In other words, high privacy concerns raised in the early stages of platform adoption may eliminate social norm, which is still weak, causing possibly a platform adoption collapse. On the other hand, early and low privacy concerns may outweigh social norm temporarily, causing only a delay in platform adoption. In addition, for high values of T^0PC, relatively high values of privacy concerns are required to have an impact on social norm, which becomes stronger as platform adoption takes place. Thus, the earlier the privacy concerns start, the easier it is for privacy concerns to outweigh social norm, hence making the paradox less likely, and vice versa.

6 Concluding discussion

This article presents a system dynamics simulation model that considers the diversity of privacy concerns during the process of social media adoption and identifies the types of situations in which the privacy paradox emerges. The model illustrates that (1) the least concerned minority can induce the more concerned majority to adopt social media and (2) even the most concerned minority can be hindered by the less concerned majority from discarding social media. Both (1) and (2) are types of situations that reflect the privacy paradox.

Since the model was built as a generic representation of social media, a limitation of the simulation results is that they do not apply exactly to every platform and context. As such, a fruitful topic for future research would be to empirically test and validate the simulation results and thus support the usefulness and applicability of the model both in the context of specific social media platforms and in additional contexts, such as peer-to-peer (P2P) platforms like Airbnb and Uber. Finally, the model could be developed further to study the privacy paradox in the context of platform competition. For example, the model could include two or more platforms and therefore identify the types of situations in which people may continue to use platforms that were launched early but face privacy issues (e.g. WhatsApp) or decide to switch to privacy alternatives that were launched later (e.g. Signal).

Acknowledgements

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

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

Appendix: Model equations and parameter values

The model equations and parameter values are shown in Table A1. In the equations, subscript w refers to the user group (p: Pragmatists, f: Fundamentalists, u: Unconcerned). The model includes formulations to ensure that users cannot be added or removed spontaneously (i.e. mass balance) and that stock variables stay non-negative. For clarity, these have been omitted from the equations shown in Table A1. For details of the formulations and to ensure the replicability of the simulation results, the simulation model Vensim file is openly available upon request.

References

1. Arzoglou, E., Kortesniemi, Y., Ruutu, S., Elo, T.: The Role of Privacy Obstacles in Privacy Paradox: A System Dynamics Analysis (Submitted) (2022)
2. Barlas, Y.: Formal Aspects of Model Validity and Validation in System Dynamics. System Dynamics Review **12**(3), 183–210 (1996)
3. Bass, F.M.: A New Product Growth for Model Consumer Durables. Management Science **15**(5), 215–227 (1969)
4. Brown, B.: Studying the Internet Experience. HP Laboratories Technical Report 49 (2001)
5. Casey, T.R., Töyli, J.: Dynamics of Two-Sided Platform Success and Failure: An Analysis of Public Wireless Local Area Access. Technovation **32**(12), 703–716 (2012)
6. Choi, H., Park, J., Jung, Y.: The Role of Privacy Fatigue in Online Privacy Behavior. Computers in Human Behavior **81**, 42–51 (2018)
7. Dienlin, T., Trepte, S.: Is the Privacy Paradox a Relic of the Past? An In-Depth Analysis of Privacy Attitudes and Privacy Behaviors. European Journal of Social Psychology **45**(3), 285–297 (2015)
8. van Dijck, J.: Facebook and the Engineering of Connectivity: A Multi-Layered Approach to Social Media Platforms. Convergence **19**(2), 141–155 (2013)
9. Kokolakis, S.: Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. Computers and Security **64**, 122–134 (2017)
10. Rosenberg, R.S.: The Social Impact of Computers. Academic Press Inc. (1992)
11. Ruutu, S., Casey, T., Kotovirta, V.: Development and Competition of Digital Service Platforms: A System Dynamics Approach. Technological Forecasting and Social Change **117**, 119–130 (2017)
12. Statista: Special Eurobarometer 447 - Online Platforms (2016), `https://www.statista.com/study/37575/social-networks-search-engines-and-online-marketplaces-in-the-eu-28/`
13. Sterman, J.D.: Business Dynamics: Systems Thinking and Modeling for a Complex World. McGraw-Hill (2000)
14. Westin, A.F.: Privacy and Freedom. Atheneum (1967)
15. Westin, A.F.: Social and Political Dimensions of Privacy. Journal of Social Issues **59**(2), 431–453 (2003)

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47

Table A1. Model equations and parameter values

Name		Equation/parameter value	Unit	#
Potential users	$\dot{P_w}$	$= DR_w - AR_w$	User	1
	$P_w(0)$	$= 1000$		
Users	$\dot{U_w}$	$= AR_w - DR_w$	User	2
	$U_w(0)$	$= 0$		
Adoption rate	AR_w	$= P_w \cdot (a + c \cdot af_w \cdot U_w/N_w)$	User/Year	3
Discard rate	DR_w	$= U_w \cdot df_w/\tau$	User/Year	4
Adoption fraction	af_w	$= V_w/(V_w + V^*)$	-	5
Discard fraction	df_w	$= V^*/(V^* + V_w)$	-	6
Total population	N_w	1000 (divided into 550 Pragmatists, 250 Fundamentalists, and 200 Unconcerned)	User	
Advertising start time	T^0	0	Year	
Advertising end time	T	4	Year	
Advertising effectiveness	a	0.01	1/Year	
Contact rate	c	10	1/Year	
User reaction time	τ	1.5	Year	
User fraction	uf_w	$= U_w/N_w$	-	7
Reference user fraction	uf^*	0.5	-	
Platform value	V_w	$= (\frac{\sum_w uf_w}{uf^*})^\gamma + E_w$	-	8
Reference value	V^*	3	-	
Effect of users on platform value	γ	0.7	-	
Privacy concerns (Pragmatists)	PC_p	$= PC(0)-$ Step $(P^*, T^0 PC)$ Step input function	-	9a
Privacy concerns (Fundamentalists)	PC_f	$= PC(0)-$ Step $(P^* \cdot F^*, T^0 PC)$ Step input function	-	9b
Privacy concerns (Unconcerned)	PC_u	$= PC(0)-$ Step $(P^* - (P^* \cdot U^*), T^0 PC)$ Step input function	-	9c
Reference privacy concerns	PC_w^*	$=$ Smoothi $(PC_w, \tau PC, PC(0))$ Exponential smoothing function	-	10
		$= PC(0)$ (no erosion of privacy concerns)		10′
Privacy concerns initial value	$PC(0)$	0	-	
Privacy concerns start time	$T^0 PC$	5	Year	
Privacy concerns erosion time	τPC	5	Year	
Reference pragmatism	P^*	0.5	-	
Reference fundamentalism	F^*	3	-	
Reference unconcern	U^*	0.5	-	
Effect of privacy concerns on platform value	E_w	$= PC_w - PC_w^*$	-	11

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08751-6_47