Alternative platforms and privacy paradox: A system dynamics analysis

Ektor Arzoglou and Yki Kortesniemi

Department of Information and Communications Engineering, Aalto University, Helsinki, Finland
{ektor.arzoglou,yki.kortesniemi}@aalto.fi

Abstract. The term 'privacy paradox' refers to the apparent inconsistency between privacy concerns and actual behaviour that also often leads to the dominance of privacy-careless over privacy-respecting platforms. One of the most important explanations for this phenomenon is based on the concept of social norm, which refers to the influence that an individual's social environment can have on their decisions to accept or reject a specific platform. However, the interdependencies between social norm dynamics and platform adoption have received little attention so far. To overcome this limitation, this article presents a system dynamics simulation model that considers the concept of social norm, shaped by users with diverse privacy concerns, during the adoption process of two alternative social media platforms and identifies the types of situations in which the privacy paradox emerges. The results show a bidirectional minority rule, where (1) the least concerned minority can hinder the more concerned majority from discarding a privacy-careless platform but also (2) the most concerned minority can induce the less concerned majority to adopt a privacy-respecting platform. Both (1) and, to a lesser extent, (2) are types of situations that reflect the privacy paradox.

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

1 Introduction

Digital platforms act as *mediators* of content flows between users. In addition, they typically tailor this content to individual user preferences (i.e. personalisation) based on the processing of accumulated user data. At the same time, the repeated involvement of Big Tech platform owners (e.g. Alphabet and Meta) in cases of user data exploitation has raised privacy concerns, thereby motivating the launch of privacy-respecting platforms, such as the search engine DuckDuckGo and the instant messenger Signal, which were introduced as alternatives to Google Search and WhatsApp, respectively.

Over the last decade, researchers have started to investigate the role of privacy concerns in the adoption of online services, such as digital platforms, by usually assuming that privacy concerns will likely result in rejection of privacy-careless platforms. However, these studies neglect that, despite expressing high

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

privacy concerns, people may still choose a privacy-careless over a privacy-respecting platform. This inconsistency between privacy concerns and actual behaviour is often referred to as the *privacy paradox* [10].

One of the most important explanations for this phenomenon is based on the concept of *social norm*, which refers to the influence that an individual's social environment can have on their privacy decisions. As a result, individuals may *conform* to the social norm by deciding to accept the use of a platform that they would otherwise reject in order to achieve approval from and harmony with peers and family regardless of privacy preferences and concerns [3]. Social norm is a *dynamic* concept that influences individual behaviour while also being shaped by mass behaviour over time [8]. In addition, it is not necessarily aligned with privacy protection, because it might be shaped by people with less need for privacy and therefore low privacy concerns. Diffusion (i.e. the spread of an innovation through a population) theory [12] and social psychology [1] suggest that more careful attention to the social context should be paid in order to understand the determinants of innovation adoption. However, the concept of social norm has often been modelled as a *static* parameter in innovation diffusion models. This limitation motivates the development of a *system dynamics simulation model* [15] that presents an *endogenous* perspective (i.e. arising from within the system) on the social norm concept in this article.

The research question guiding this article is: *In what types of situations can a social norm outweigh privacy concerns, when choosing from two alternative social media platforms, and how does this help understand the privacy paradox?* The results of the developed system dynamics simulation model show a bidirectional *minority rule*, where (1) the least concerned minority can hinder the more concerned majority from discarding a privacy-careless platform but also (2) the most concerned minority can induce the less concerned majority to adopt a privacy-respecting platform. Both (1) and, to a lesser extent, (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 social aspects of 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 two alternative social media platforms. 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 [10, 13]. This article focuses exclusively on the third aspect.

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

2.1 Privacy as a social issue

Nissenbaum conceptualises privacy as *contextual integrity*, which is defined as "the appropriate information flows in a given context", and assumes two explicit information norms: (1) *appropriateness*, governing what information is revealed in a given context, and (2) *flow*, governing the recipients of that information in a given context. Contextual integrity is maintained when both norms are upheld and is breached, thus exacerbating privacy concerns, when either of the norms is violated. Unlike previous theories, which often view privacy as a generic and static concept cutting across different contexts, contextual integrity postulates that privacy concerns vary depending on the context [11].

An important implication, which may also explain the privacy paradox, of defining privacy as contextual integrity is that it reveals the *key difference between "giving up" privacy and giving up information*. That is, users do not cede their privacy by sharing their data if they perceive the information flow as appropriate for that specific context. Hence, users may express high privacy concerns before using a service and also retain these concerns while using the service, which they expect to respect the norms governing the recipients of and rights over a certain piece of information.

This implication may apply to single-purpose contexts (e.g. e-commerce platforms, such as Alibaba), in which users enact pre-defined roles and also information sharing is governed by explicit norms. However, it does not apply to multi-purpose contexts (e.g. social media platforms, such as Instagram), in which roles are ever changing and likely unknown a priori (i.e. relationships among users are constantly evolving) and also information norms are implicit (i.e. they encourage behaviour that is consistent with the most common behaviour). In addition, studies show that privacy concerns stem from uncertainty about both data collection by the platform (i.e. violation of appropriateness) and exploitation by third parties (i.e. violation of flow). Finally, feelings of exhaustion and cynicism towards privacy, generated from inability to meet privacy goals, may ultimately lead to a state of resignation about privacy (i.e. "giving up" privacy) and potentially to the inconsistency between privacy concerns and actual behaviour that indicates the privacy paradox [7].

2.2 Social theory based explanations of the privacy paradox

Most individuals are not autonomous in their decisions to accept or reject the use of a specific platform, since these decisions are often driven by the need to achieve conformity with the admired peer groups [8]. As such, individuals may conform to the influence of their social environment by neglecting privacy concerns in order to reap the benefits of belonging to a community rather than facing the costs (e.g. social stigmas) of being excluded from the community (i.e. positive net platform value).

In addition, social interactions are categorised into *Gemeinschaften* (communities), determined by internalised emotional ties and implicit rules (i.e. norms), and *Gesellschaften* (societies), determined by rational calculations and explicit

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

rules (i.e. laws) [16]. Certain types of platforms, such as media sharing (e.g. YouTube) and knowledge (e.g. Reddit) platforms, have both a Gemeinschaft side, where people share private information because this is an implicit rule of belonging to a community, but also a Gesellschaft side, where people know explicitly, albeit on an abstract level, and become concerned about the privacy risks based on the platforms' formal rules and policies. Hence, the dominant side is often the Gemeinschaft side, since the concrete and immediate benefits of belonging to a community outweigh the abstract privacy risks of data sharing (i.e. positive net platform value).

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* [15]. 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.

Researchers have only recently started to study the privacy paradox by focusing on the interdependencies between social norm dynamics and platform adoption [2, 3]. However, these studies focus on the adoption process of a *single* privacy-careless platform, thereby neglecting whether and how a privacy-respecting alternative could at least partially resolve the privacy paradox. To overcome this limitation, this article presents a system dynamics simulation model that considers the concept of social norm, shaped by users with diverse privacy concerns, during the adoption process of *two* alternative social media platforms and identifies the types of situations in which the privacy paradox emerges.

In system dynamics, the model development begins by (1) defining *reference modes*, which are graphs illustrating the problem (e.g. the privacy paradox) as a pattern of behaviour over time, and (2) formulating 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 [15].

3.1 Problem articulation and dynamic hypothesis

In order to illustrate the privacy paradox in the context of two alternative social media platforms, this article uses two reference modes relevant to platform adoption: an initial period of growth in adoption of the privacy-careless platform is followed by a decline, during which adoption of the privacy-respecting platform either (1) increases without ultimately dominating (e.g. the privacy-careless platform can maintain a larger fraction of highly concerned users, who are hindered by less concerned users from discarding) or (2) increases and ultimately dominates (e.g. the privacy-respecting platform can obtain a larger fraction of less concerned users, who are induced by highly concerned users to adopt). On one

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

hand, reference mode (1) illustrates a situation in which privacy concerns are inconsistent with adoption of the privacy-careless platform, thus reflecting the privacy paradox. On the other hand, although reference mode (2) illustrates a situation in which privacy concerns are consistent with adoption of the privacy-respecting platform, the privacy paradox is reflected again, but this time to a lesser extent.

The purpose of the model is to explain the types of situations in which a social norm can outweigh privacy concerns using these two 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.

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) [6], can produce the two modes of dynamic behaviour. As such, platform adoption can be influenced by different factors (e.g. privacy concerns) that have an effect on the feedback loops of the model. The dynamics of the two alternative social media platforms are generated *endogenously* (i.e. from within the system). Conversely, the dynamics of privacy concerns, which can be described as a merely negative concept not bound to any specific context [9,10], are generated *exogenously* (i.e. from without the system).

4 Model development

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. Intermediate variables between stocks and flows indicate *auxiliaries*, which essentially clarify the sequence of events that cause the flows to change the stocks. Finally, a circular sequence of variables related by causal links forms a *feedback loop*, which can be either *reinforcing* (R) (i.e. amplifying change) or *balancing* (B) (i.e. counteracting and opposing change).

4.1 Model structure

The two alternative social media platforms are modelled by extending the Bass model of innovation diffusion, which considers adoption through exogenous efforts, such as advertising, and adoption through word-of-mouth [6] (Figure 1). Here, potential users can adopt either one of the two platforms. Both platforms are represented by the same model structure, but each platform is represented by a different subscript (see Appendix). Finally, the model utilises several equations from Ruutu et al. [14].

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

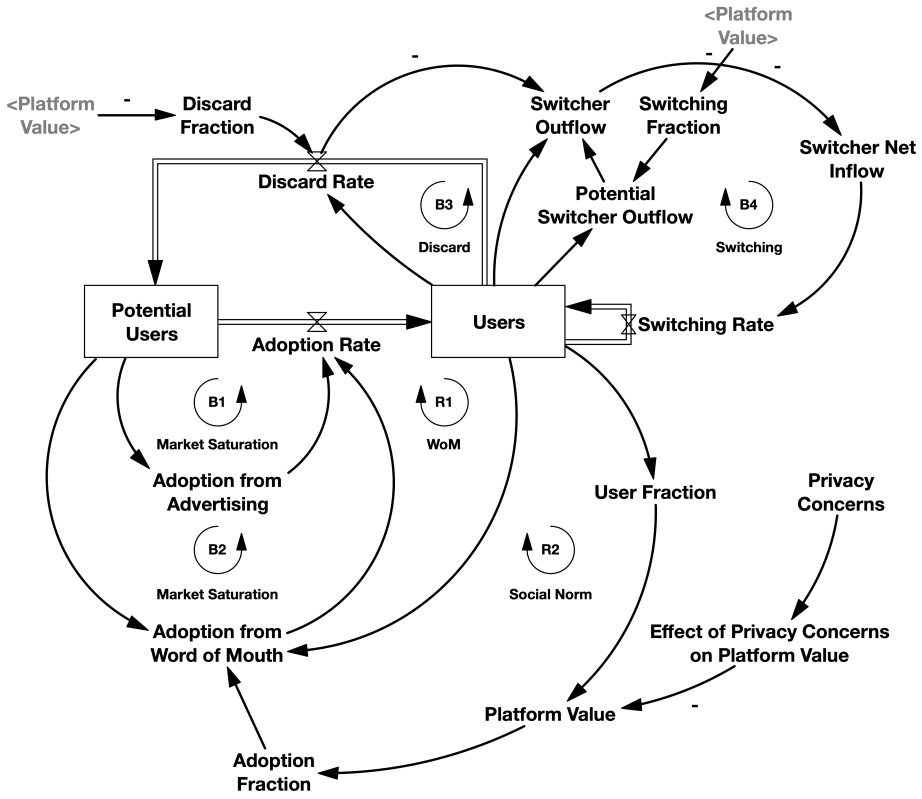

Fig. 1. Social media adoption affected by social norm and privacy concerns

When a 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 (B3: "Discard") or switch to an alternative (B4: "Switching"), depending on the decrease, caused by privacy concerns, in platform value.

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 adoption of the two platforms will progress, and

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

they make their decisions regarding platform adoption, discard, and switching 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 as per Westin's first privacy segmentation into 550 Pragmatists (mid to high privacy concerns P^*), 250 Fundamentalists (high privacy concerns F^*), and 200 Unconcerned (no or low privacy concerns U^*) [17]. In this regard, F^* is a multiplier of P^*, and U^* can range from zero ($U^* = 1$) to matching P^* ($U^* = 0$).

Furthermore, $PC(0)$ determines the initial value of privacy concerns, and T^0PC determines the time at which privacy concerns start. The effect of privacy concerns on platform value erodes (using exponential smoothing) over time τPC. This erosion essentially indicates the time for users to develop either (1) feelings of exhaustion, resignation, and even cynicism towards privacy (i.e. privacy fatigue) [7] or (2) feelings of privacy safety [5]. 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. Initially, an external advertising effort (a), starting at time T^0 and ending at time T, brings the first users in the platform. Thereafter, potential users come into contact (c) with current users, and platform adoption continues only with word-of-mouth. Conversely, it takes some time (τ) for users to process the decrease, caused by privacy concerns, in platform value and react by discarding the platform or switching to an alternative. Moreover, V^* determines the value that users receive from substitutes, and uf^* determines the fraction of users needed in order to obtain the same level of benefits. Therefore, high values of these two parameters make platform adoption harder. Finally, exponent γ determines the strength of social norm (i.e. the dependency of platform value 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. The validation tests that have been successfully passed to gradually build confidence in the soundness and usefulness of the model, with respect to the purpose presented in Section 3, are grouped into *direct structure tests*, which do not involve simulation, and *structure-oriented behaviour tests*, which involve simulation [4]. The results are presented in Table 1.

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

Table 1. 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 [6].
Parameter confirmation	All parameters in the model (1) have clear and meaningful counterparts in the real world and (2) 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 users cannot be added or removed spontaneously (i.e. mass balance) and that stock variables 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 (e.g. no users, no 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.

5 Simulation results

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

5.1 Simulation experiment 1

For the first simulation experiment (Figure 2), platform 1 is launched at $Time = 0$ and platform 2 is launched two years later ($Time = 2$). In platform 1, Fundamentalists are one point two times as concerned as Pragmatists ($P^* = 0.1$, $F^* = 1.2$), on the assumption that privacy preferences of Fundamentalists are somewhat stronger. In addition, Unconcerned are less than one third as concerned as Pragmatists ($U^* = 0.7$), 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. On the other hand, in platform

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

2, all three user groups are two fifths as concerned as in platform 1 (P^*, F^*, $U^* = 0.4$), assuming that platform 2 is more than twice as private as platform 1 but still not perfectly private. In addition, erosion of privacy concerns applies to all three user groups, on the assumption that users realise the privacy benefits and feel safer about their data over time.

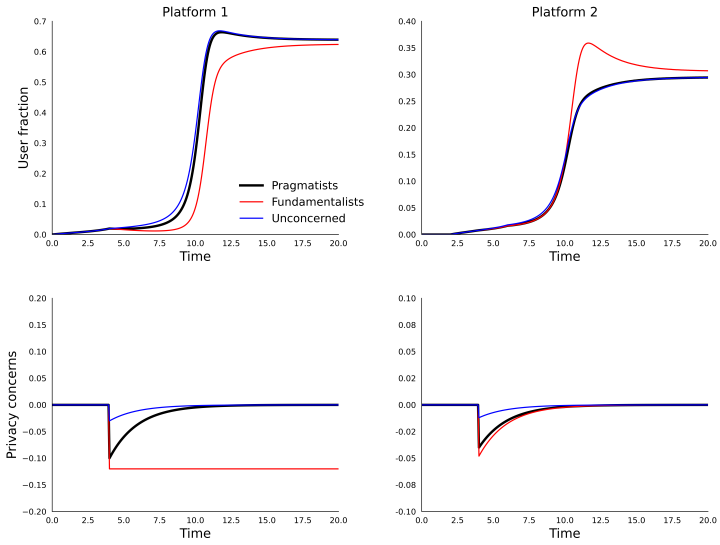

Fig. 2. The social norm created by Pragmatists and Unconcerned results in adoption of platform 1 also for a larger fraction of Fundamentalists, although privacy concerns of the last user group remain constant.

For both platforms, adoption initially takes place through advertising (B1) and word-of-mouth (B2, R1). Advertising efforts (B1) last four years (ending at $Time = 4$ for platform 1 and $Time = 6$ for platform 2), and platform adoption continues only with word-of-mouth (B2, R1) thereafter. Moreover, privacy concerns start at $Time = 4$ in both platforms for all three user groups. At this point, in platform 1, social norm (R2) outweighs privacy concerns of Unconcerned but is outweighed by privacy concerns of Pragmatists and Fundamentalists, thus preserving platform value and adoption only for the first user group. By contrast, the number of Pragmatists and Fundamentalists is starting to decline. On the other hand, in platform 2, social norm (R2) outweighs privacy concerns of all three user groups, and therefore platform adoption increases. As a result, from $Time = 5.5$ until $Time = 10.5$, platform 1 maintains a larger fraction of Pragmatists and Unconcerned, despite the decline of the first user group, while platform 2 obtains a larger fraction of Fundamentalists, who have switched from platform 1. However, as the number of Unconcerned grows and also privacy concerns of Pragmatists erode in platform 1, social norm (R2) outweighs privacy

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

concerns of the second user group, and therefore the number of Pragmatists is once more starting to grow ($Time = 6$). At the same time, adoption of platform 2 increases, but the installed user base remains smaller compared to platform 1. In other words, the social norm (R2) driving adoption of platform 1 outweighs the social norm (R2) driving adoption of platform 2. Finally, as the number of both Pragmatists and Unconcerned grows in platform 1, social norm (R2) becomes strong enough to eventually outweigh privacy concerns of Fundamentalists too. As a result, the number of Fundamentalists starts to grow again ($Time = 9$), although privacy concerns of this user group do not erode, and platform 1 ultimately dominates platform 2.

The first simulation experiment illustrates a *minority rule that prevents change*, since the smallest user group of Unconcerned initially hinders the largest user group of Pragmatists, before both eventually hinder the user group of Fundamentalists, from switching to platform 2. In addition, although (1) privacy concerns of Pragmatists are not eliminated in platform 1, (2) privacy concerns of Fundamentalists remain constant in platform 1, and (3) platform 2 is more than twice as private as platform 1, a larger fraction of Pragmatists and Fundamentalists eventually adopts platform 1, hence resulting in the privacy paradox. Finally, the results of the first simulation experiment are also consistent with the results of Arzoglou et al. [2].

5.2 Simulation experiment 2

The setup of the second simulation experiment (Figure 3) is similar to the first, with the only difference being that privacy concerns of Fundamentalists erode faster in platform 2 ($\tau PC_f = 1$). The assumption is that Fundamentalists are more literate about privacy and therefore able to realise the privacy benefits sooner than Pragmatists and Unconcerned.

As before, privacy concerns start at $Time = 4$ and while the number of Pragmatists and Fundamentalists declines, the number of Unconcerned continues to grow in platform 1. In addition, by $Time = 10.5$, a larger fraction of Fundamentalists has already switched to platform 2, whereas a larger fraction of Pragmatists and Unconcerned remains again in platform 1. However, as the number of Fundamentalists grows in platform 2, the social norm (R2) driving adoption of platform 2 eventually outweighs the social norm (R2) driving adoption of platform 1. As a result, all three user groups switch to platform 2, which ultimately dominates platform 1.

The second simulation experiment illustrates a *minority rule that drives change*, since a smaller user group of Fundamentalists induces a larger user group of Pragmatists and Unconcerned to switch to platform 2. In addition, although privacy concerns of Fundamentalists remain constant, a smaller fraction of this user group eventually adopts platform 1, thus exhibiting again the privacy paradox, but this time to a lesser extent.

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

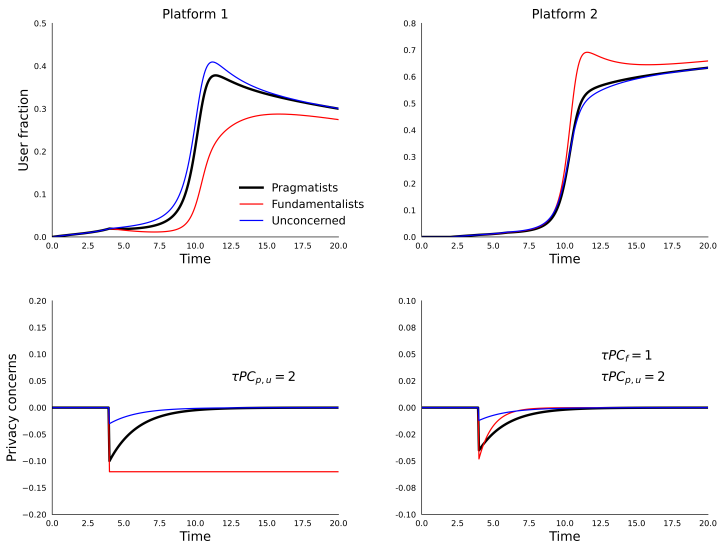

Fig. 3. The social norm created by Fundamentalists results in adoption of platform 2 also for a larger fraction of Pragmatists and Unconcerned.

5.3 Simulation experiment 3

For the third simulation experiment (Figure 4), platform 1 is launched at $Time = 0$ and platform 2 is launched at time $Time = 5$, which is one year after privacy concerns start for platform 1 ($Time = 4$). The assumption is that the privacy issues of platform 1 motivate the launch of platform 2. In platform 1, Fundamentalists are two times as concerned as Pragmatists ($P^* = 0.1$, $F^* = 2$), on the assumption that privacy preferences of Fundamentalists are significantly stronger. In addition, Unconcerned are one half as concerned as 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, once more on the assumption that Fundamentalists are less likely to feel privacy fatigued over time. On the other hand, all three user groups have no privacy concerns in platform 2, which is assumed to be perfectly private.

Again, privacy concerns start at $Time = 4$, and the number of Pragmatists and Fundamentalists declines in platform 1. At the same time, the number of Unconcerned continues to grow, although privacy concerns of this user group are higher compared to the previous two simulation experiments. On the other hand, adoption of platform 2 starts at $Time = 5$ and increases at the highest possible rate. Similar to the first simulation experiment, the number of Unconcerned is sufficient to initially hinder Pragmatists from discarding platform 1. However, contrary to the first simulation experiment, adoption of platform 1 from Pragmatists and Unconcerned becomes easier only when privacy concerns of the two

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

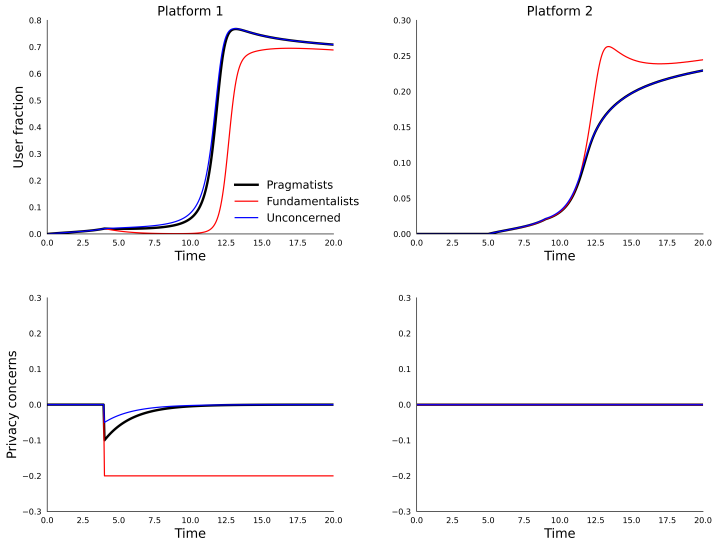

Fig. 4. The social norm created by Pragmatists and Unconcerned results in adoption of platform 1 also for a larger fraction of Fundamentalists, although privacy concerns of the last user group remain constant.

user groups are nearly eliminated. In other words, the social norm (R2) driving adoption of platform 1 outweighs the social norm (R2) driving adoption of platform 2, but this dominance is counterbalanced by the effect of privacy concerns on the value of platform 1. For this reason, adoption of platform 1 increases only when the effect of privacy concerns on the value of platform 1 becomes weaker. Finally, as the number of both Pragmatists and Unconcerned grows in platform 1, social norm (R2) becomes strong enough to eventually outweigh privacy concerns of Fundamentalists too. As a result, the number of Fundamentalists starts to grow again ($Time = 11$), although privacy concerns of this user group do not erode, and platform 1 ultimately dominates platform 2.

For the third simulation experiment, the minority rule and privacy paradox for all three user groups are similar to the first simulation experiment. In addition, the results of the third simulation experiment are also consistent with the results of Arzoglou et al. [2].

6 Concluding discussion

This article presents a system dynamics simulation model that considers the concept of social norm, shaped by users with diverse privacy concerns, during the adoption process of two alternative social media platforms and identifies the types of situations in which the privacy paradox emerges. The model illustrates a bidirectional minority rule, where (1) the least concerned minority can hinder

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

the more concerned majority from discarding a privacy-careless platform but also (2) the most concerned minority can induce the less concerned majority to adopt a privacy-respecting platform. Both (1) and, to a lesser extent, (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 to specific platforms across different contexts. Finally, the model could be developed further to present an endogenous perspective on the concept of privacy concerns, determined by e.g. the users' data sharing behaviour and the platform's exploitation of accumulated user data.

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), and subscripts i and j refer to the two alternative social media platforms. For clarity, the equations are shown without the formulations that ensure the validity of stock variables (see Section 4.3). 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. Ajzen, I., Fishbein, M.: The Prediction of Behavior from Attitudinal and Normative Variables. Journal of Experimental Social Psychology **6**(4), 466–487 (1970)
2. Arzoglou, E., Kortesniemi, Y., Ruutu, S., Elo, T.: Privacy Paradox in Social Media: A System Dynamics Analysis. In: Groen, D., de Mulatier, C., Paszynski, M., Dongarra, J.J., Sloot, P.M.A. (eds.) Computational Science - ICCS 2022. Lecture Notes in Computer Science, vol. 13350, pp. 651–666. Springer, Cham (2022)
3. Arzoglou, E., Kortesniemi, Y., Ruutu, S., Elo, T.: The Role of Privacy Obstacles in Privacy Paradox: A System Dynamics Analysis. Systems **11**(4), 205 (2023)
4. Barlas, Y.: Formal Aspects of Model Validity and Validation in System Dynamics. System Dynamics Review **12**(3), 183–210 (1996)
5. Bartsch, M., Dienlin, T.: Control Your Facebook: An Analysis of Online Privacy Literacy. Computers in Human Behavior **56**, 147–154 (2016)
6. Bass, F.M.: A New Product Growth for Model Consumer Durables. Management Science **15**(5), 215–227 (1969)
7. Choi, H., Park, J., Jung, Y.: The Role of Privacy Fatigue in Online Privacy Behavior. Computers in Human Behavior **81**, 42–51 (2018)
8. Cialdini, R.B., Trost, M.R.: Social Influence: Social Norms, Conformity and Compliance. In: The Handbook of Social Psychology, pp. 151–192. McGraw-Hill (1998)
9. 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)

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

10. Kokolakis, S.: Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. Computers and Security **64**, 122–134 (2017)
11. Nissenbaum, H.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford Law Books (2009)
12. Rogers, E.M.: Diffusion of Innovations. Free Press (2003)
13. Rosenberg, R.S.: The Social Impact of Computers. Academic Press Inc. (1992)
14. 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)
15. Sterman, J.D.: Business Dynamics: Systems Thinking and Modeling for a Complex World. McGraw-Hill (2000)
16. Tönnies, F.: Community and Society. Dover Publications (2003)
17. Westin, A.F.: Social and Political Dimensions of Privacy. Journal of Social Issues **59**(2), 431–453 (2003)

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12

Table A1. Model equations and parameter values

Name		Equation/parameter value	Unit	#
Potential users	$\dot{P_w}$	$= \sum_i (DR_{w,i} - AR_{w,i})$	User	1
	$P_w(0)$	$= 1000$		
Users	$\dot{U_{w,i}}$	$= AR_{w,i} + SR_{w,i} - DR_{w,i}$	User	2
	$U_{w,i}(0)$	$= 0$		
Adoption rate	$AR_{w,i}$	$= P_w \cdot (a + c \cdot af_{w,i} \cdot U_{w,i}/N_w)$	User/Year	3
Discard rate	$DR_{w,i}$	$= U_{w,i} \cdot df_{w,i}/\tau$	User/Year	4
Switching rate (from j to i)	$SR_{w,i}$	$= \sum_j (U_{w,j} \cdot sf_{w,j,i} - U_{w,i} \cdot sf_{w,i,j})/\tau$	User/Year	5
Adoption fraction	$af_{w,i}$	$= V_{w,i}/(\sum_i V_{w,i} + V^*)$	-	6
Discard fraction	$df_{w,i}$	$= V^*/(V^* + \sum_i V_{w,i})$	-	7
Switching fraction (from i to j)	$sf_{w,i,j}$	$= V_{w,j}/(\sum_i V_{w,i} + V^*)$ (0 if $i = j$)	-	8
Total population	N_w	1000 (divided into 550 Pragmatists, 250 Fundamentalists, and 200 Unconcerned)	User	
Advertising start time	T^0	0, 2 (platform 2 is launched later)	Year	
Advertising end time	T	4, 6	Year	
Advertising effectiveness	a	0.01	1/Year	
Contact rate	c	10	1/Year	
User reaction time	τ	1.5	Year	
User fraction	$uf_{w,i}$	$= U_{w,i}/N_w$	-	9
Reference user fraction	uf^*	0.5	-	
Platform value	$V_{w,i}$	$= (\frac{\sum_w uf_{w,i}}{uf^*})^\gamma + E_{w,i}$	-	10
Reference value	V^*	2.2	-	
Effect of users on platform value	γ	0.7	-	
Privacy concerns (Pragmatists)	$PC_{p,i}$	$= PC(0)_i -$ Step (P_i^*, T^0PC_i) Step input function	-	11a
Privacy concerns (Fundamentalists)	$PC_{f,i}$	$= PC(0)_i -$ Step $(P_i^* \cdot F_i^*, T^0PC_i)$ Step input function	-	11b
Privacy concerns (Unconcerned)	$PC_{u,i}$	$= PC(0)_i -$ Step $(P_i^* - (P_i^* \cdot U_i^*), T^0PC_i)$ Step input function	-	11c
Reference privacy concerns	$PC^*_{w,i}$	$=$ Smoothi $(PC_{w,i}, \tau PC, PC(0)_i)$ Exponential smoothing function	-	12
		$= PC(0)_i$ (no erosion of privacy concerns)		12′
Privacy concerns initial value	$PC(0)_i$	0	-	
Privacy concerns start time	T^0PC_i	4	Year	
Privacy concerns erosion time	τPC	2	Year	
Reference pragmatism	P^*	0.1, 0.4 (platform 2 is more private)	-	
Reference fundamentalism	F^*	1.2, 0.4	-	
Reference unconcern	U^*	0.7, 0.4	-	
Effect of privacy concerns on platform value	$E_{w,i}$	$= PC_{w,i} - PC^*_{w,i}$	-	13

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-35995-8_12