Not a Paradox: Revisiting the Personalization-Privacy Relationship as an Assemblage

Shruti Sharma
Ph.D. Research Scholar,
Symbiosis International (Deemed University)
India-411057
Shruti0203@gmail.com

Dr. Adya Sharma
SCMS, Symbiosis International (Deemed University)
Viman Nagar, Pune, India-411014
adyaindia@gmail.com

Abstract

Recognizing ever changing contexts and resultant interactions are imperative to generate novel perspectives. Personalization-privacy relationship has been treated as a paradox and this constructed perpetual polarity, disguising the fact that they are two sides of the same coin and working in the same environment. With devices increasingly becoming personal, expectations of users have increased too, which paved way for hyper-personalization. It creates the need to revisit and re-evaluate privacy paradox notion. Embracing privacy issues as a constraint of business would lead towards practical solutions. This paper dives deep in the assumptions of paradox using problematization method and proposes an alternative view of it as an assemblage. It is argued that these mutually interactive and evolving elements should be comprehended in assemblage rather than in isolation. Once it is accepted as process, different efforts can be put towards better framing of privacy statements and for awareness too. This paper contributes towards exploring new perspectives with changing times, which is a core principle of building knowledge and this paper provides a fresh perspective for novel enquiries and actions.

***Keywords**:* Privacy; Paradox; Personalization; Assemblage theory; Problematization

Not a Paradox: Revisiting the Personalization-Privacy Relationship as an Assemblage

1. Introduction

Changing user preferences demand better engagement, more than just behavioural targeting. Addressing them with personalization is important to the customers as well as marketers. Personalization, as a term, has been used in literature to describe variety of actions. Personalization is a collection of fragmented ideas like segmentation, targeting and customisation, based on context, data used and initiator of it (Strycharz, van Noort, Helberger, & Smit, 2019). Users want to be considered more, 48% of users prefer to be distinct and more selective. They are pressed for time more than ever and so the expectations of engagement have also been transformed. Instant gratification and smooth stress-free experiences which suits efficiency-driven lives are most welcome (Euromonitor, 2019). Loads of options and information coupled with time pressed lifestyle makes a strong case for preference-based targeting. Too many options are desirable and attractive initially but there is resultant frustration with decision-making process and dissatisfaction afterwards (Iyengar & Lepper, 2000).

Employing technological advances to ensure a simple and efficient path to purchase has become essential, rather than optional. Online Behavioural advertising has been effective in closing transactions, if advertisements are less but more relevant; helps in reducing information overload and is received positively by the user (Strycharz et al., 2019). Benefits of personalization do exist for users as well as practitioners. Awad and Krishnan (2006) speculated that a fraction of users is of privacy fundamentalists (Westin, 2003), who are unwilling to value personalization irrespective of the privacy features implemented by the firms. Xu, Luo, Carroll, & Rosson (2011) studied privacy concerns in context of location aware marketing and found that relevant and contextual personalization is considered valuable and somehow outweighs privacy concerns. Users' need greater control, transparency over how the data is used; while being fascinated by novelties that help them avoid queues, save time, synchronise and organize their personal information and preferences (Euromonitor, 2019). This makes obvious for the firms to focus their efforts towards larger category of privacy pragmatists and privacy unconcerned category who are willing to participate in personalization (Awad & Krishnan, 2006; Westin, 2003). Every business would try to woo the target audience and reduce irrelevant advertising, which further brings advantages like increased revenues, better click and response rates, loyal users, higher persuasion. Personalization can alter behavioural intentions of users and reduce acquisition costs by increasing marketing efficiency, which increases revenue too (Ariker, Heller, Diaz, & Perrey, 2015). Businesses are ready to spend more for lesser, but right targeted advertising, which is beneficial to both advertisers and costumers. Relatively weak impact of personalization is observed in case of preference mismatch whereas relevant content made user attitudes positive (Sundar & Marathe, 2010). Even after targeting right person at right time, quality of content or recommendation is

ISSN 2348–0661 Print

valued and inevitably rich data profiles are needed to achieve the same (Lee & Cranage, 2011), which bring privacy concerns into the picture.

Norberg, Horne,and Horne (2007) established the term "*privacy paradox*" as the relationship between intentions and actual behaviour towards personal information disclosure, where it was found that users freely provided personal data despite having complaints (Sutanto, Palme, Tan, & Phang, 2013; Bandara, Fernando, & Akter, 2020). The term paradox conveys numerous and wide-ranged meanings. It has been often used to explain conflicting demands, polarizing notions, or apparently illogical findings; though labelling them as paradox does not essentially promote understanding of phenomenon. Even human existence has been viewed as paradoxical, due to tensions between life and death (Lewis, 2000). "*It's a paradox*" has become overused and underspecified. The whole thing is paradox that way, reward of efficient production is boosted consumption (Beam, 1994). The notion of privacy paradox was referenced initially to describe the baffling divide in connection with social networking sites, where youngsters were sharing private lives online without comprehending its implications but older generations were fighting for privacy (Barnes, 2006); however, this assumption about youngsters that they are not protective of their private information has been challenged (Blank, Bolsover, & Dubois, 2014).

This paper contests the notion of privacy paradox and posits that privacy is a constraint in hyper-personalization environment, but not a paradox. Shifting the efforts from preventing data collection to data usage and handling may lead towards better solutions and renewed investigations. This paper uses qualitative enquiry to capture the relative nature (Sofaer, 1999) of the personalization-privacy relationship and contributes in bringing the focus towards the potential positive impact of changing perspective towards privacy issues. Problematization method (Alvesson & Sandberg, 2011) is used to contest the privacy paradox notion and an alternative view of it as an assemblage (Deleuze & Guattari, 1995; DeLanda, 2015) is proposed.

This paper is organized further as follows: Conceptual background of various explanations of paradox in brief is discussed, then problematization method is described. Concept of privacy is understood to contest the notion of paradox. Then, alternative view of personalization-privacy assemblage is proposed, followed by discussion.

2. Conceptual background

Consumers share ample information in practice and various explanations are provided for such behaviour. The inconsistency in privacy attitudes and privacy behaviour, termed as paradox, is interpreted with help of social theory, psychology, behavioural economics and quantum theory. Focus of current privacy paradox research is on construing the gap between privacy attitude and privacy behaviour (Kokolakis, 2017). Concept of privacy is subjective and privacy paradox has been interpreted through various theoretical lenses. Some of the conclusions are following from literature on privacy paradox explanation.

Decision making in real world is largely influenced by wealth frame or by gains and losses (Kahneman, 2003). Users' intention to reveal personal information is based on cost-benefit trade-

ISSN 2348–0661 Print

off where they want most positive and least negative consequences (Knijnenburg et al., 2018; Pappas, 2018), try to maximize benefits and minimize cost (Fife & Orjuela, 2012), or evaluate risks against the gains to be received, like more customized deals and discounts. This outlook treats privacy as a quantifiable commodity (Aguirre, Roggeveen, Grewal, & Wetzels, 2016). Privacy calculus theory has been used widely to understand privacy behaviours of users who trade part of privacy in exchange for perceived benefits which they consider worth the risk of information disclosure (Dinev & Hart, 2006). Privacy trade-off in mobile app context becomes more specific as smartphones have become self-extensions and very personal to user and also, a permanent company (Wottrich, van Reijmersdal, & Smit, 2018). Mobile applications offer many values or perceived benefits to users like social interaction, information search, entertainment and shopping. Even if user is aware of privacy risks and safety procedures, they might be unable to take rational privacy-sensitive decisions (Wottrich et al., 2018). A reluctance to pay in monetary terms indicate disposition of consumer to provide information as the cost of receiving benefits or services. Free apps are downloaded more often than paid ones (Fife & Orjuela, 2012). Receiving personalization benefits like better recommendations, communication and overall better experience include bearing costs like privacy risk, spams, unintended price differentiations and many more (Strycharz et al., 2019). Xu et al. (2011) also supports the notion of users balancing value and risk.

Concept of privacy is dependent on cultures too and there is no coherent view over personal privacy globally. One personal information which may be acceptable in one culture, may be despised in another (Fife & Orjuela, 2012). Online social networks have been entrenched in social lives which persuades users for self-disclosure despite their privacy concerns (Blank et al., 2014); the desire of being part of a community bumps with the calculated risk of data misuse. Individual decisions about information sharing are heavily influenced by contextual factors, which underscores importance of social context and stresses that human behaviour is a significantly derived from unconscious motivation (Kokolakis, 2017).

Flender and Müller (2012) uniquely engaged quantum theory concepts to explain the privacy paradox. Human decision-making is considered similar to the measurement process in quantum experiments which incorporates perspective of indeterminacy. It proposes that decision making outcomes are affected by indeterminacy effect where preferences of individuals are decided at the time of decision but not prior to it. Bandara et al. (2020) explained privacy paradox as an outcome of a value-conflict based on Construal level theory of psychological distance. Privacy as a high-construal and psychologically-distant central value is undermined by low-construal, immediate, and proximal secondary value such as shopping gratification. Feasibility of proximal choices takes over the desirability of distant privacy protection psychologically. Users' superseding desire to install app diminishes their cognizance to permission requests and jargon-based permission requests are difficult for regular users to understand; one possible explanation is given by present bias theory, wherein people neglect future cost and prefer instant gratification (O'Donoghue & Rabin, 2015). Human decision making is not consistent and does not always seek utility maximization. Individual choices are shaped by their existent or non-existent knowledge and their

ISSN 2348–0661 Print

capacity or lack of it, to use the knowledge when it is needed, while coping with uncertainty and competing demands. Bounded rationality constrains human ability to obtain and utilize information (Simon, 2000). Taking cue from framework of contextual integrity, exploring role of contextualization holds much importance. Contextualization of privacy paradox implies that privacy concerns vary across individuals as well as circumstantial factors (Gu, Xu, Xu, Zhang, & Ling, 2017). Another interesting study by Dienlin and Trepte (2015) showed that using different research models and methodological approaches can lead to contradictory results and dissolve privacy paradox.

After going through key explanations, it is imperative to consider that digital environment has proliferated quickly. Smartphones are a companion now which break the time-space matrix, brings ubiquity, convenience, immediacy and continuity to user. Devices are evolving and so are the users. The pertinent question here to ask is, "*if the phenomenon of paradox is still the same*"? Interactive nature of smart objects and their ability "*to affect and be affected*" (Hoffman & Novak, 2018) has been overlooked in context of users. User experiences are formed through repeated interactions over time and each repeated interaction is different than previous one (Hoffman and Novak, 2018). This paper attempts to evaluate the privacy paradox by understanding the initial presumptions about it and if they still stand valid. With passing time and changing environment, some assumptions may lose their relevance to drive novel enquiries. Gadamer (2004) called them "*prejudices about the subject matter in question*".

3. Contesting the paradox notion

Numerous explanations are being given to explain the "why" of paradox and this paper contests this notion using problematization as a methodology (Alvesson & Sandberg, 2011). Qualitative methods allows us "not only to describe events but to understand how and why the same events are often interpreted in a different, sometimes even conflicting manner, by different stakeholders" (Sofaer, 1999). Generally, research questions are generated by identifying or constructing gaps in existing knowledge, which is a dominant method in management. Though gap-spotting research is important to develop existing knowledge, many editors of reputed journals have vociferously raised issue of lack of research, which are consensus challenging and present new or alternate ways of thinking. Challenging assumptions may be risky and chances of publication are reduced (Starbuck, 2011). Gap spotting and problematization are not mutually exclusive but two distinct ways of asking questions. With this method, this paper embraces general meta-theoretical stance that all knowledge is uncertain (Kuhn, 2012) and problematization methodology is used here to ask question through a dialectical interrogation targeted for assumption challenging (Alvesson & Sandberg, 2011). Problematization is an "endeavour to know how and to what extent it might be possible to think differently, instead of what is already known" (Foucault, 1985). Problematization questions the presumptions which were used to develop the concept as knowledge production uses some assumptions as starting point. Problematizer not only need to question the assumption, but is required to provide an alternative viewpoint too. One methodological tactic to identify assumption is to view something negative or repressive as neutral. Andrews, Andrews, Luo, Fang,

ISSN 2348–0661 Print

and Ghose (2016) explored positive aspect of crowding wherein people turned inwards and immersed themselves in their mobile devices to avoid negative emotions like anxiety which resulted in increased response for mobile ads in crowded subway environment. Recognition of multiple values, interest and contradictions can be beneficial. To debunk the notion of paradox, it is imperative to grasp concept of privacy first.

Privacy is discussed in literature from various aspects. Privacy is rooted in fundamental characteristic of social life and social structure creates context. An information which is freely available in one social circle like family can be embarrassing as an employee. "*What is or should be private*" is purely contextual and one single standard cannot be applied to judge it (Blank et al., 2014). Privacy has been mainly viewed as a right, as a commodity, as control, and as limited access to one's information (Martin & Murphy, 2017). Individual privacy is reflective of specific needs and desires which constantly changes and is function of life situation based on family life, education, social class, and psychological makeup. Westin (1968) described four states of individual privacy; solitude, intimacy, anonymity, and reserve which also change constantly. Varying personal needs and choices make privacy a complex condition, and privacy can signify different things to different people and it extends beyond just data secrecy (Solove, 2020), (Westin, 2003). In online scenario, Personal data includes direct or indirect identifiable information of an individual like, IP addresses, digital fingerprinting, location data (Goddard, 2017).

Difference in stated and revealed preference of users led to coinage of the term privacy paradox, but is it really a paradox? Paradox as a noun can be understood as a situation *"having seemingly contradictory qualities or phases"* or *"an argument that apparently derives self-contradictory conclusions by valid deduction from acceptable premises"*(Merriam-Webster, 2021). Paradox represents interrelated but contradictory elements, which are logical in isolation but irrational when put together (Lewis, 2000). Theory of Constraints suggests that every business aspires to earn money, now and in future both, and anything that creates barrier or limits the performance of business to achieve that goal can be called a constraint (Gupta & Boyd, 2008). Privacy can be treated as an operational constraint towards hyper-personalization. To contest existing notion, understanding and asking questions about its assumptions is imperative. If researchers considered it to be a paradox, what assumptions did they make? Is that assumption still useful? This paradox continues similarly like expanding individual freedom, brings along dependencies with it (Wisman, 1995). This paper contests the notion that personal information "*should not to be shared*" as it is the "*right thing*" to do, is an ideological stance, which shows in stated preferences of users. It needs to be upgraded to, "*sharing what is needed*" is fine. This shift in stance is supported by arguing for decoupling of data usage concerns from data collection. Also, we elucidate that flawed constructs, privacy fatigue and a brief existence of learning paradox have contributed in creating a notion of paradox.

ISSN 2348–0661 Print

3.1. **Decoupling data usage and data collection**

The possible misuse of information is actually the fundamental threat to individual privacy rather than information collection. Consumers might share their information while having general concerns for privacy, but with expectations that information will be used within the norms of the context of exchange (Bandara et al., 2020). It indicates that people are fine with sharing data to enjoy personalization and better services, which should not be labelled as apathy towards privacy. Nissenbaum (2009) argued that only practices which support unbecoming flow of personal information, infringe user's perception of privacy. As one respondent in study of Rainie and Duggin (2016) puts it, "*The data isn't really the problem. It's who gets to see and use that data that creates problems*". The phrase which captured views best about privacy and personal information disclosure in their study is, "*It depends*". Polykalas and Prezerakos (2019) found that there is no correlation between amount of data access extent and number of app installations which indicates that data access is not a barrier for installation. Once user perceives benefits as adequate, relevant data collection or certain intrusiveness is taken as proper (Wottrich et al., 2018). Various studies support the notion that data collection is not the source of privacy concern but the usage is. Sutanto et al. (2013) proposed an IT solution to soothe privacy concerns and found that the users are fine with giving data and taking services but their concerns are about usage and sharing of their data. It is noteworthy that despite apprehensions and concern, users are giving data to use services, which indicates that benefits trump all apprehensions and it is re-iterated in many studies (Xu et al., 2011).

Privacy is not only about personal data protection; it is more about protecting users' autonomy, individuality, identity, ability to make mistakes without worry, with the assurance that their steps would not be followed and prevention from unpredictable negative consequences of those mistakes (Strycharz et al., 2019). As guided by Fair Information Practice Principles (Culnan & Armstrong, 1999), any information collector should inform users about the reason and subsequent management of collected information. Authority of an individual to decide what self-information should be known to others including the control of when such information will be acquired and how it will be used by others. Thus, decoupling data usage and data collection has to be done (Lee & Cranage, 2011) as users are concerns about the later only.

3.2. **Flawed constructs and analysis**-

Contextualism and behaviourism dominate the privacy research. Behavioural intentions are nothing but the resultant output of belief and action outcome evaluation (Ajnen, 1991) and contrary beliefs can co-exist. People who want to lose weight desperately become impulsive and eat cheese burger when it is presented to them. Exposure to tasty food increases cravings (Houben, Nederkoorn, & Jansen, 2012). They sure want to stick to diet, they can see cheese, read calorie label but still they eat it. Is it a cheese burger paradox? Or simply a case of preferred behaviour versus actual behaviour. Attitude and behaviour are fundamentally different, their difference cannot be termed as paradox. Behaviour implies risk decisions within specific contexts and is always contextual whereas attitudes are generic views about value which are beyond specific

ISSN 2348–0661 Print

contexts. So, the diversion in the attitude and behaviour about privacy is not a paradox (Solove, 2020). User make choice to achieve a certain goal and going through "*constructive consumer choice processes*", it is found that, four significant goals are about maximum choice accuracy, minimum cognitive effort, minimum negative emotion, and maximum comfort in justifying the decision (Bettman, Luce, & Payne, 1998). As noted above, these goals find place in paradox explanations too. All the explanations of paradox are actually explaining the actual behaviour, stated behaviour can be more understood as an ideological stance or attitude of doing the "right thing".

Moreover, privacy paradox studies are mostly based on surveys and experiments. Self-reported behaviour in surveys is inadequate to capture actual behaviour, and experiments lack in creating a genuine context of individual behaviour (Kokolakis, 2017). When privacy concerns are viewed as contextual, behaviour prediction becomes challenging (Aguirre et al., 2016). Inadequacies of study designs or different methodological approach can also be a crucial source behind mis-conceptualization of privacy behaviour as a paradox. Individuals may not behave the same as they would in normal contextual scenario, even though the experiment details given to them are false (Kokolakis, 2017). Using same sample and survey instrument, Dienlin and Trepte (2015) tested privacy paradox with two different methods. Their second approach dissolved the privacy paradox and established that contradictory results appear by using alternative methods of analysis and research models.

3.3. **Briefly experienced learning paradox**-

It is imperative to consider "*timing*", as an assumption might be productive and inspiring sometime but may lose its sheen over time as a driver of rethinking (Alvesson & Sandberg, 2011). Times have changed in terms of indispensability of smart objects and relevant personalization. The emergence of consumer-object assemblages strongly indicates that smart objects play a role in consumption-related processes. Human-centric outlook may be limiting prospects of addressing important questions about the future of consumer behaviour (Hoffman & Novak, 2018). Smart objects', especially smartphones' anytime-anywhere feature is a big differentiator. The object-oriented anthropomorphism (Hoffman & Novak, 2018) has changed behaviour towards this ubiquitous and self-extension like object. Smartphones are not only the device to provide comfort but has become much more like extension of self (Melumad & Pham, 2020). The immersion in technology and benefits of it skew the cost benefit trade-off towards benefits. As McLuhan (1964) famously stated, "*Medium is the message*". More than content, characteristics of the medium mould the behaviour. Smartphones have become indispensable and this indispensability stems from micro-level practices of daily routines which leads to ritualization of activities. If a product is very utilitarian and functional at one extreme or at the other extreme very symbolic with great personal significance, then it becomes indispensable (Hoffman, Novak, & Venkatesh, 2004). Smartphones are portable, provide psychological comfort, haptic pleasure, give sense of privacy and are highly personal. It reassures its presence in daily lives of consumers not only because of functionalities but due to unique combination of properties (Melumad & Pham, 2020). Agarwal & Karahanna (2000) defined cognitive absorption as "*a state of deep involvement with software*"

ISSN 2348–0661 Print

and smartphones fulfil all five dimensions of it; namely, temporal dissociation (no track of time), focused immersion (other attentional demands are neglected), heightened enjoyment (pleasant aspects), control (user's perception of being in charge), curiosity (aroused sensory and cognitive curiosity). Smartphones are moving from touch to a multisensory experience with augmented reality and virtual reality which results in better user experiences, visual and emotional appeal (Mishra, Shukla, Rana, & Dwivedi, 2021). Smart devices are evolving beyond simple data collection and supporting hyper-personalization. They are learning through the interaction with users and getting better at it with the help of artificial intelligence. The data from smart, connected products offers a sharper image about product usage or non-usage of features. Finer segmentations can be created by analysing usage patterns and better pricing strategies and value can be offered even to the individual user (Porter & Heppelmann, 2015).

Technology proliferation has been dramatic and rapid. Initially, it may cause learning paradox where old assumption or beliefs are not adjusted to new environments. In Cannon's words, "*Paradoxes emerge when beliefs or assumptions fail to keep up with external changes*" (Cannon, 1996). Actors may even neglect need of learning and use cognitive and behavioural frames to construct support for their view. Splitting as a strategy to resolve paradox further polarize conflicts due to artificial distinctions that mask similarities. Defensive behaviour towards this learning paradox might have initially to reduce the frustrations and discomfort of tensions, actors' defensive behaviours initially yielded positive outcomes but ultimately foster opposite effects which deepen the underlying tension (Lewis, 2000).

3.4. **Case of privacy fatigue**

Considering privacy, a commodity or placing monetary value on personal data is incapable and inaccurate as a metric to produce meaningful outcome, as it might reflect a risk assessment of personal data but not its value. When privacy is viewed as a right, as a commodity, and as limited or controlled information access, information sharing by individuals is assumed as relinquishing of expectation of privacy (Martin & Murphy, 2017).

People are not able to self- manage their privacy and if they choose to share personal data for any price, it is a reflection of their inability and resignation rather that of the value of the data (Solove, 2020). Explosion of privacy-invasive technologies have limited the ability of users to protect their information. Moreover, even after taking up this arduous task of privacy protection, it is not achievable. Privacy boundaries are repeatedly invaded and users perceive that they have lost authority over their information, then they give-up on protecting their privacy (Bandara et al., 2020). This state of resignation cannot be termed as apathy towards privacy concerns. Users have to cross the crucial stage while downloading any app which is accept permission request (Wottrich et al., 2018). Technical jargon of permission is hard to understand for users and they are more inclined to finish task; even if few users understand it, they are not aware about the consequences (Gu et al., 2017). Out of many business models like paid, freemium, in-app advertising models, completely free apps monetize user data by means of advertising or by selling non-personal data (Tang, 2019); and Yale Privacy Lab detected trackers in over 75% of android apps. Various data

ISSN 2348–0661 Print

like location, contact list, device content and personally identifiable information, like user names were tracked and shared with third parties (Sean & Kwet, 2017).

Tang, Akram, & Shi (2020) explores role of "*privacy fatigue*" while taking information sharing decisions. Privacy fatigue has two dimensions; powerlessness (emotional exhaustion) and numbness (cynicism) caused by privacy issues. Updating password, complex "*terms and conditions*", Internet of Things (IoT) environment affect users and as a result, after reaching fatigue state, intention to protect privacy significantly declines. While using personalized offers, user makes a choice between personalization benefits and privacy risk (Pappas, 2018). Users show eagerness to install and ignore a pop-up from app; and are not aware of consequences of it (O'Donoghue & Rabin, 2015). Privacy fatigue signifies boredom and weariness and result in reluctance to actively manage and control personal information whereas cynicism describes state of frustration, hopelessness. Privacy concerns can prompt negative consumer actions like giving false information and spreading negative word-of-mouth. Advanced data collection methods are incomprehensible for users to perform correct cost-benefit analysis and covert information collection complicates it further. Due to privacy fatigue, the split between actual and preferred behaviour might have widened even more to support pseudo paradox notion.

4. Personalization-Privacy Assemblage

4.1. **Understanding Assemblage**

Assemblage is a "*gathering of heterogeneous elements consistently drawn together as an identifiable terrain of action and debate*" (Li, 2007). Deleuze and Guattari originally used French word "*agencement*" which is translated in English as "*assemblage*". These words have different etymological roots. An assemblage is a collection of things into unities whereas an agencement is a layout of heterogenous forces or elements (Nail, 2017), (DeLanda, 2015). As an assemblage is created, at the core of it, agencement lies. An assemblage is comprised of heterogeneous elements or forces, often considered disparate or separate whose concord comes purely from the fact that they work towards or in same environment to bring something in being which may be a policy or a resultant force (Feely, 2020), (Baker & McGuirk, 2017).

An assemblage claims a territory which is attained through ongoing processes of stabilization and destabilization (Wise, 2018). It emphasizes on active connection, combination and alignment of relations between heterogeneous element. Thus, assemblage thinking is popular and has been applied to fields as diverse as public participation, urban development practices, industrial production. Roy (2012) observed that "*the analytics of assemblage has come to pose important methodological questions for the social sciences*" and stressed that an assemblage explain the existence and relation of things. Assemblage methodologies are guided by epistemological commitments which denote an interrogative orientation (Baker & McGuirk, 2017).

ISSN 2348–0661 Print

4.2. **Creating framework**

An assemblage is always in a fitting process and analysis of an assemblage entails investigating how elements are doing it (Youdell, 2010). Context-rich descriptions of elements are required (Davies & Riach, 2018) to form assemblage. This methodological-analytical approach follows a three-stage process to answer this question (Feely, 2020). Firstly, identifying the disparate components or forces which create the phenomenon. Personalization and privacy, as concrete elements, are present in an environment, where multiple social, legal, political, and business factors influence them. They need to be viewed together and not in silos to understand the resultant. Secondly, assemblages are made of and impact flows of various orders. They have an operational logic that can be mapped (Baker & McGuirk, 2017).

These elements are coded according to their usage in assemblage, i.e., as per the conditions and requirements, they can change their limits. For example, Deleuze and Guattari showed that "*the house is segmented according to its rooms' assigned purposes, streets, according to the order of the city; the factory, according to the nature of the work and operations performed in it*" (Deleuze & Guattari, 1995). Territorial assemblages operate itinerantly , change happens progressively, one concrete point at a time (Nail, 2017). Further, a "*Binary Territorial Assemblage"* is created as it suits the nature of elements and their resultant balancing force which influences decision outcome.

In this binary, elements cannot be studied independently as they form an organic mechanism. This assemblage fulfils all three conditions of elements to form an assemblage, namely; conditional context, concrete elements and their connection. Utility of using digital platform is the connecting point of both elements. The concept is nested and interrelated with other issues which make its environment (e.g. social, legal, regulatory, digital environment) and are important to investigate the meaning arising from these relations (Kitchin, Lauriault, & Wilson, 2017). Changes in environment pave way for change within the assemblage, but ultimately destabilization is followed by stabilization and assemblage is retained. These elements are advantaged or disadvantaged by particular contexts and it re-emphasizes importance of context. Identification of disparate elements, establishment of process flow, recognition of forces from element to maintain assemblage, and uncertainties of destabilization are four epistemological commitments (Baker & McGuirk, 2017), which are followed in constructing this assemblage.

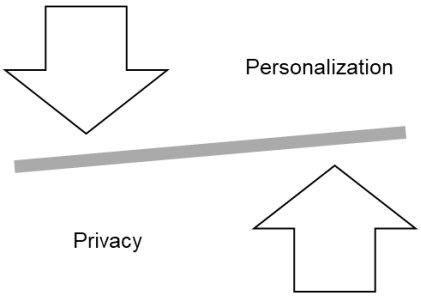

Figure 1. Personalization-privacy assemblage

ISSN 2348–0661 Print

5. Discussion

Creating something new is possible on either white canvas or after scraping the used one to remove existing accumulated layers. It is similar in case of concepts, where accumulated layers of cliché have to be scraped to pave way for novel enquiries. Changes in users' perspective with time and indispensability of smart objects have to be considered. The notion of personal information "*is not to be shared*", is an ideological stance. It is an accepted or "*correct thing to do*" but actual behaviour varies from it and falsely termed as paradox. As this term was coined, numerous explanations were offered which actually explained actual behaviour. This notion is contested based on the change of time, impact of methodologies and analytical approaches, privacy fatigue and the possibility of it briefly being a learning paradox due to quick proliferation of technology. The endeavour to contribute novel perspective towards the treatment of personalization-privacy relationship flourished in presenting this relationship as an assemblage, using problematization as a method. This paper tries to answer the question, if challenging this assumption is useful? Certainly yes. It is an endeavour to think differently than what is already known. It is essential to rethink and challenge fundamental assumptions to pave way towards more interesting and influential theories (Alvesson & Sandberg, 2011). Further, as users move towards hyper-personalization and smart connected world, information disclosures must be embraced as a process. An assemblage is an organic mechanism, which keeps changing as per environmental influences, i.e., stabilization and destabilization of elements are the continuous processes. Resultant impact of forces is understood better in an assemblage as it takes repeated interactions and its influence in account.

This assemblage underlines the organic interactions and affects, these elements have on each other, as every interaction is evolving and different than previous one. It is advocated not to view them as isolated elements. The assemblage highlights those negative consequences of personalization are nothing but misuse of data. Data collection as a process is simultaneously influenced by elements of assemblage. This data is used for personalization and results in better products or services. Same data can be misused and may result in discriminant pricing or fraudulent behaviours like identity theft and money frauds. Guns, processed food, cigarettes and numerous things were made for varied reasons like security, satiety, convenience and pleasure, yet there exist unintended consequences like murder, obesity and cancer. The unintended consequences totally depend on the usage. Many things which are started with good intention, turn ugly without proper handling. Technologies like augmented reality, virtual reality, internet of things would soon become widespread and if that many things will associate with smartphones, personal information collection would be a need and norm. All it requires is, judicious handling of data.

If firms would decide everything, from data collection to storage, to usage; they would use it in every possible way to maximize profits. It makes a strong case for privacy regulations as they exist in other business areas of food safety, drug, industrial waste and so on. General Data Protection Regulation (GDPR) for European Union (General Data Protection Regulation, 2016) is a step in right direction (Goddard, 2017) and should be followed worldwide. As the regulations

ISSN 2348–0661 Print

and policies are available for guidance, solutions will be worked on like Truong, Sun, Lee, & Guo (2020) presents blockchain based solution for personal data management. Generally, firms opposed complete privacy regulation, with the view of it being a needless interference (Westin, 2003), but with changing times, business leaders are advocating privacy as a human right too. One core thing about privacy debate is data usage and right over it. Though it may not be absolute, it would be bound by some conditions. Even the law of self-defence, which is natural and absolute (Ashworth, 1975) is bound by principles like reasonable avoidance of conflict or withdrawing from place or situation. People are sharing information with zeal. For example, a person declared on Facebook that he is out of city for a full week holiday and house is locked. A burglar liked his post and happily performed a burglary (Srinivas, 2018). This draws attention towards creation of responsibilities and awareness in data sharing too. Common sense should prevail as no law can substitute that.

An assemblage underscores need of regulation, decouples data usage from data collection, recognises presence of environmental influence. It is to be recognised that digital platforms proliferated quite quickly, to provide users with enriched experiences. Without proper regulations and guidance, data and privacy issues became awful. Similar to other fields, embracing issues as a part of business, a challenge, or an operational constraint, would augment the solution seeking. Debunking the privacy paradox might shift focus on data usage stream of research and evolution of different codes of usage and various territories may gather traction. Acceptance of data collection as norm would shift focus on sensitising, researching and regulating the usage of data.

6. Concluding Remarks

There are no predefined answers available, new questions offer starting points for new answers. This paper endeavoured to propose a fresh perspective by contesting 'privacy paradox' as popular notion and takes stance that data collection is the need, and privacy issues are nothing but business constraints. It is suggested to be neutral towards privacy issues. There are many aspects to an assemblage, which might have been left out. Future researchers can dive deep in details to envisage this relationship with more clarity. Emphasis on filling intention-action gap in privacy research is important for responsible technology development. Future research topics can include determining most direct environmental factors influencing the assemblage, providing better model, measuring the quantity of impact, examining the reasons about the stated privacy response, specifying stabilization and destabilization forces and case studies about.

References

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly: Management Information Systems*, *24*(4), 665–694. https://doi.org/10.2307/3250951

Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: implications for new media. *Journal of Consumer Marketing*, *33*(2), 98–110. https://doi.org/10.1108/JCM-06-2015-1458

ISSN 2348–0661 Print

Ajnen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Alvesson, M., & Sandberg, J. ¨ O. (2011). GENERATING RESEARCH QUESTIONS THROUGH PROBLEMATIZATION. *Academy of Management Review*, *36*(2), 247–271. https://doi.org/10.5465/amr.2009.0188

Andrews, M., Andrews, M., Luo, X., Fang, Z., & Ghose, A. (2016). Mobile ad effectiveness: Hyper-contextual targeting with crowdedness. *Marketing Science*, *35*(2), 218–233. https://doi.org/10.1287/mksc.2015.0905

Ariker, M., Heller, J., Diaz, A., & Perrey, J. (2015). How Marketers Can Personalize at Scale. *Hbr.Org*, 2–6. Retrieved from https://hbr.org/2015/11/how-marketers-can-personalize-at-scale

Ashworth, A. J. (1975). Self-defence and the right to life. *The Cambridge Law Journal*, *34*(2), 282–307. https://doi.org/10.1017/S0008197300086128

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly: Management Information Systems*, *30*(1), 13–28. https://doi.org/10.2307/25148715

Baker, T., & McGuirk, P. (2017). Assemblage thinking as methodology: commitments and practices for critical policy research. *Territory, Politics, Governance*, *5*(4), 425–442. https://doi.org/10.1080/21622671.2016.1231631

Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, *52*. https://doi.org/10.1016/j.jretconser.2019.101947

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9), 5. https://doi.org/10.5210/fm.v11i9.1394

Beam, H. H. (1994). The Age of Paradox. *Academy of Management Perspectives*, *8*(2), 94–96. https://doi.org/10.5465/ame.1994.9503101152

Bettman, J. R., Luce, M. F., & Payne, J. W. (1998). Constructive consumer choice processes. *Journal of Consumer Research*, *25*(3), 187–217. https://doi.org/10.1086/209535

Blank, G., Bolsover, G., & Dubois, E. (2014). *A New Privacy Paradox: Young People and Privacy on Social Network Sites*. *Proceedings of the Annual Meeting of the American Sociological Association*. https://doi.org/10.2139/ssrn.2479938

Buchanan, I. (2021). *Assemblage Theory and Method*. *Assemblage Theory and Method*. https://doi.org/10.5040/9781350015579

Cannon, T. (1996). *Welcome to the Revolution: Managing Paradox in the 21st Century*. Retrieved

from https://research.usc.edu.au/discovery/fulldisplay/alma993665902621/61USC_INST:ResearchRepository

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Davies, O., & Riach, K. (2018). Sociomateriality and Qualitative Research: Method, Matter and Meaning In: The SAGE Handbook of Qualitative Business and Management Research Methods: Methods and Challenges Sociomateriality and Qualitative Research: Method, Matter and Meaning. https://doi.org/10.4135/9781526430236

DeLanda, M. (2015). *Assemblage Theory*. *Edinburgh university press*. Retrieved from https://edinburghuniversitypress.com/pub/media/wysiwyg/pdfs/samples/DeLanda-Assemblage_Theory-Introduction.pdf

Deleuze, G., & Guattari, F. (1995). A Thousand Plateaus. *SubStance*, *20*(1), 117. https://doi.org/10.2307/3684887

Dienlin, T., & Trepte, S. (2015). 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. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Euromonitor. (2019). Top 10 Global Consumer Trends For 2019. *Euromonitor International*, (March). Retrieved from http://www.portal.euromonitor.com/portal/analysis/tab

Feely, M. (2020). Assemblage analysis: an experimental new-materialist method for analysing narrative data. *Qualitative Research*, *20*(2), 174–193. https://doi.org/10.1177/1468794119830641

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management*, *4*(1), 1–10. https://doi.org/10.5772/51645

Flender, C., & Müller, G. (2012). Type indeterminacy in privacy decisions: The privacy paradox revisited. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 7620 LNCS, pp. 148–159). https://doi.org/10.1007/978-3-642-35659-9_14

Foucault, M. (1985). The use of pleasure. In *New York* (Vol. 2). Retrieved from http://books.google.com/books?id=rKy9QgAACAAJ&pgis=1

Gadamer, H.-G. (2004). *Truth and Method*. *Bloomsbury Publishing USA*. Bloomsbury Publishing USA. https://doi.org/10.5840/philstudies19762551

General Data Protection Regulation. (2016). General Data Protection Regulation (GDPR) – Official Legal Text. Retrieved February 25, 2021, from https://gdpr-info.eu/

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6). https://doi.org/10.2501/IJMR-2017-050

Gu, J., Xu, Y. (Calvin), Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19–28. https://doi.org/10.1016/j.dss.2016.10.002

Gupta, M. C., & Boyd, L. H. (2008). Theory of constraints: a theory for operations management. *International Journal of Operations & Production Management*, *28*(10), 991–1012. https://doi.org/10.1108/01443570810903122

Hoffman, D. L., & Novak, T. P. (2018). Consumer and object experience in the internet of things: An assemblage theory approach. *Journal of Consumer Research*, *44*(6), 1178–1204. https://doi.org/10.1093/jcr/ucx105

Hoffman, D. L., Novak, T. P., & Venkatesh, A. (2004). Has the Internet become indispensable? *Communications of the ACM*, *47*(7), 37–42. https://doi.org/10.1145/1005817.1005818

Houben, K., Nederkoorn, C., & Jansen, A. (2012). Too tempting to resist? Past success at weight control rather than dietary restraint determines exposure-induced disinhibited eating. *Appetite*, *59*(2), 550–555. https://doi.org/10.1016/j.appet.2012.07.004

Iyengar, S. S., & Lepper, M. R. (2000). When Choice is Demotivating: Can One Desire Too Much of a Good Thing? *Journal of Personality and Social Psychology*, *79*(6), 995–1006. https://doi.org/10.1037/0022-3514.79.6.995

Kahneman, D. (2003). A Perspective on Judgment and Choice Mapping Bounded Rationality. https://doi.org/10.1037/0003-066X.58.9.697

Kitchin, R., Lauriault, T. P., & Wilson, M. W. (2017). *Understanding Spatial Media*. *Understanding Spatial Media*. https://doi.org/10.4135/9781526425850

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H. (2018). Death to the Privacy Calculus? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2923806

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kuhn, T. S. (2012). *The Structure of Scientific Revolutions*. University of Chicago press.

Lee, C. H., & Cranage, D. A. (2011). Personalisation-privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism*

Management, *32*(5), 987–994. https://doi.org/10.1016/j.tourman.2010.08.011

Lewis, M. W. (2000). Exploring paradox: Toward a more comprehensive guide. *Academy of Management Review*, *25*(4), 760–776. https://doi.org/10.5465/AMR.2000.3707712

Li, T. M. (2007). Practices of assemblage and community forest management. *Economy and Society*, *36*(2), 263–293. https://doi.org/10.1080/03085140701254308

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4

McLuhan, M. (1964). Understanding media: The extensions of man. *MIT Press.* https://doi.org/10.1016/j.plrev.2011.10.017

Melumad, S., & Pham, M. T. (2020). The Smartphone as a Pacifying Technology. *Journal of Consumer Research*, *47*(2), 237–255. https://doi.org/10.1093/jcr/ucaa005

Merriam-Webster. (2021). Paradox | Definition of Paradox by Merriam-Webster. Retrieved January 21, 2021, from https://www.merriam-webster.com/dictionary/paradox

Mishra, A., Shukla, A., Rana, N. P., & Dwivedi, Y. K. (2021). From "touch" to a "multisensory" experience: The impact of technology interface and product type on consumer responses. *Psychology & Marketing*, *38*(3), 385–396. https://doi.org/10.1002/mar.21436

Nadella, S. (2019). Privacy is a human right, we need a GDPR for the world: Microsoft CEO. In *World Economic Forum*. Retrieved from https://www.weforum.org/agenda/2019/01/privacy-is-a-human-right-we-need-a-gdpr-for-the-world-microsoft-ceo/

Nail, T. (2017). What is an Assemblage? *SubStance*, *46*(1), 21–37. Retrieved from https://muse.jhu.edu/article/650026

Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. In *Privacy in context: Technology, policy, and the integrity of social life.* https://doi.org/10.1080/15536548.2011.10855919

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

O'Donoghue, T., & Rabin, M. (2015). Present bias: Lessons learned and to be learned. In *American Economic Review* (Vol. 105, pp. 273–279). American Economic Association. https://doi.org/10.1257/aer.p20151085

Pappas, I. O. (2018). User experience in personalized online shopping: a fuzzy-set analysis. *European Journal of Marketing*, *52*(7–8), 1679–1703. https://doi.org/10.1108/EJM-10-2017-0707

Polykalas, S. E., & Prezerakos, G. N. (2019). When the mobile app is free, the product is your

personal data. *Digital Policy, Regulation and Governance* , *21*(2), 89–101. https://doi.org/10.1108/DPRG-11-2018-0068

Porter, M. E., & Heppelmann, J. E. (2015). How Smart, Connected Products Are Transforming Companies. Harvard Business Review.

Rainie, L., & Duggin, M. (2016). Privacy and Information Sharing. *Pew Research Center Internet Project*, *15*(December 2015), 47. Retrieved from http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/

Roy, A. (2012). Ethnographic circulations: Space-time relations in the worlds of poverty management. *Environment and Planning A*, *44*(1), 31–41. https://doi.org/10.1068/a44180

Sean, O., & Kwet, M. (2017). Mobile Trackers | Yale Privacy Lab. Retrieved July 17, 2020, from https://privacylab.yale.edu/trackers.html

Simon, H. A. (2000). Bounded rationality in social science: Today and tomorrow. *Mind & Society*, *1*(1), 25–39. https://doi.org/10.1007/bf02512227

Sofaer, S. (1999). Qualitative methods: what are they and why use them? *Health Services Research*, *34*(5 Pt 2), 1101–1118. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/10591275%0Ahttp://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=PMC1089055

Solove, D. J. (2020). The Myth of the Privacy Paradox. *George Washington Law Review*, *89*(1), 50. https://doi.org/10.2139/ssrn.3536265

Srinivas, M. (2018). Burglar in Hyderabad likes FB posts on vacation plans, then strikes. Retrieved February 9, 2021, from https://telanganatoday.com/burglar-likes-fb-posts-on-vacation-plans-then-strikes

Starbuck, W. H. (2011). *The Production of Knowledge: The Challenge of Social Science Research*. *The Production of Knowledge: The Challenge of Social Science Research* (Vol. 173). https://doi.org/10.1093/acprof:oso/9780199288533.001.0001

Strycharz, J., van Noort, G., Helberger, N., & Smit, E. (2019). Contrasting perspectives – practitioner's viewpoint on personalised marketing communication. *European Journal of Marketing*, *53*(4), 635–660. https://doi.org/10.1108/EJM-11-2017-0896

Sundar, S. S., & Marathe, S. S. (2010). Personalization versus customization: The importance of agency, privacy, and power usage. *Human Communication Research*, *36*(3), 298–322. https://doi.org/10.1111/j.1468-2958.2010.01377.x

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly: Management Information Systems*, *37*(4), 1141–1164. https://doi.org/10.25300/MISQ/2013/37.4.07

ISSN 2348–0661 Print

Tang, A. K. Y. (2019). A systematic literature review and analysis on mobile apps in m-commerce: Implications for future research. *Electronic Commerce Research and Applications*, *37*(February), 100885. https://doi.org/10.1016/j.elerap.2019.100885

Tang, J., Akram, U., & Shi, W. (2020). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: based on personality traits. *Journal of Enterprise Information Management*. https://doi.org/10.1108/JEIM-03-2020-0088

Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security*, *15*, 1746–1761. https://doi.org/10.1109/TIFS.2019.2948287

Westin, A. F. (1968). Privacy And Freedom. *Washington and Lee Law Review*, *166*.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453. https://doi.org/10.1111/1540-4560.00072

Wise, J. M. (2018). Gilles Deleuze and Communication Studies. In *Oxford Research Encyclopedia of Communication*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228613.013.79

Wisman, J. D. (1995). The Cost of Living: How Market Freedom Erodes the Best Things in Life. *Political Science Quarterly*, *110*(3), 494. https://doi.org/10.2307/2152601

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support System*, *106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42–52. https://doi.org/10.1016/j.dss.2010.11.017

Youdell, D. (2010). *School trouble: Identity, power and politics in education*. *School Trouble: Identity, Power and Politics in Education*. https://doi.org/10.4324/9780203839379

ISSN 2348–0661 Print