In the User We Trust: Unrealistic Expectations of Facebook's Privacy Mechanisms

Conference Paper · July 2018

DOI: 10.1145/3217804.3217906

4 authors, including:

Irina Shklovski
IT University of Copenhagen
61 PUBLICATIONS **1,457** CITATIONS

SEE PROFILE

In the User We Trust: Unrealistic Expectations of Facebook's Privacy Mechanisms

Guillaume Nadon
KEA – Copenhagen Business Academy
Copenhagen, Denmark
guillaume.nadon@gmail.com

Marcus Feilberg
IT University of Copenhagen
Copenhagen, Denmark
mfei@itu.dk

Mathias Johansen
IT University of Copenhagen
Copenhagen, Denmark
mnij@itu.dk

Irina Shklovski
IT University of Copenhagen
Copenhagen, Denmark
irsh@itu.dk

ABSTRACT

Facebook has created a complex system of controls to manage disclosure in an effort to help users address privacy concerns. Do these controls work in practice? What about controls for disclosure to Facebook itself? We explore user relationships with Facebook and its privacy mechanisms using scenario building and explored their reactions. We then confronted them with their actual practices by using Facebook's apps permissions screen. While the majority of respondents felt responsible for their data disclosure, they failed to live up to their own expectations. We argue that the complexity of privacy controls places unrealistic responsibilities on the users, while masking the way Facebook itself collects user data. There is an urgent need to establish clear and explicit basic privacy norms for user relationships with social media companies.

CCS CONCEPTS

- Human-centered computing ~ Empirical studies in HCI

KEYWORDS

Privacy, user responsibility, consent, Facebook, ToS

ACM Reference format:
G. Nadon, M. Feilberg, M. Johansen, I. Shklovski 2018. In the User We Trust: Unrealistic Expectations of Facebook's Privacy Mechanisms. In Proceedings of the *International Conference on Social Media & Society*, Copenhagen, Denmark (SMSociety). DOI: 10.1145/3217804.3217906

1 INTRODUCTION

People are often left wondering how to behave as citizens in a digital world where increasingly common and large-scale data leaks [2] create concern about the impact personal data practices might have on individual lives. Ostensibly, managing personal data is an individual responsibility. Ubiquitous Terms of Services (ToS) and End User License Agreements (EULA) inform users of their rights and responsibilities. Extensive and often complicated, these texts detail the contract of data exchange into which people enter when using any digital service. Researchers have put much effort into better

[1] https://techcrunch.com/2017/09/07/equifax-data-leak-could-involve-143-million-consumers/

SMSociety '18, July 18–20, 2018, Copenhagen, Denmark
 ACM ISBN 978-1-4503-6334-1/18/07…$15.00
https://doi.org/10.1145/3217804.3217906

design of EULAs and into novel ways of assisting the user in making these decisions [39]. Few of these efforts are successful and users continue to ignore these contracts [8] in part because the complexity and time demands of becoming truly informed to make each disclosure decision remain enormous [22].

Nevertheless, millions of people share their personal data on popular social media sites every day and the volume of data is only growing. The largest and most popular digital services, such as Google and Facebook, have put significant effort into assisting their users with decisions about what data to share and how to share it, enabling a diversity of privacy control mechanisms. Facebook, with its 1.23 billion active users has worked hard to create awareness about sharing data publicly. The company has created one of the most extensive data management control dashboards and implemented a version of privacy mirrors [26] allowing users to see how others might see their content prior to publishing it [12].

Facebook has focused the majority of its privacy controls on helping users manage their disclosure to other people in their network. There are few controls available for managing how Facebook itself might utilize user data.[3] The company's business model relies on monetizing its users' information in ways that are not always made explicit. Users can control some of the advertising content they see but the reasoning and mechanics behind the classifications that users can manage is impossible to determine. This opaqueness can cause consternation as users attempt to figure out how Facebook manages to know too much about them.[4] Such consternation may lead to self-censure as users realize that in their use of Facebook they are not only disclosing information to their networks but also to Facebook itself [13].

In this paper we investigate how users think about their responsibilities for personal data, and question whether the responsibility put on them is realistic. We focus on Facebook, due its popularity and the complexity of the decisions that users must make about information disclosure given the tools Facebook makes available.

2 BACKGROUND

Concerns about privacy on social network sites (SNS) have fuelled a considerable amount of research on how users manage their identity [9], self-presentation [3], friends [14], and sharing [1] on Facebook. In discussions of data disclosure and the attendant context collapse, scholars have occasionally come to conflicting conclusions. For example, while people might use Facebook in ways similar to creating exhibits of the self, thus tightly controlling self-presentation to manage privacy [19], the site is also a tool for relational management [14] and for exchanges of support [21] – actions that could potentially lead to considerable disclosures. Despite the care that many put into deciding what to post [5,10], individual expectations of audience [6] and privacy are rarely correct [1].

Over the years, Facebook has paid close attention to research, developing features and services that address user concerns, resulting in one of the most complex and granular privacy control interfaces. Through research we know quite a bit about how people use Facebook privacy controls to manage interpersonal information disclosure [42]. Yet such disclosure controls are difficult to manage not only because of their complexity but also because of the competing pulls on our needs and our obligations [33,38]. As Vertesi et al. [38] point out, there is "a moral economy of data management" and people often feel responsible for data sharing as well as for data management.

Despite the proliferation of research, however, few scholars have paid attention to how users are engaging with the fact that their activities are disclosing their data to Facebook itself [37]. When opening a Facebook account every user has to agree to an extensive terms of service document detailing Facebook's treatment of user data. As Facebook changes this document, users are asked to agree to the changes. In effect, the user is held responsible for their decision to accept the terms of service and to enter into what essentially amounts to a commercial relationship with Facebook. The extensive terms of service and the complex outward facing privacy controls require certain epistemic capabilities from the users. The act of knowing is a prerequisite for acting responsibly [32] and knowing can only be achieved if the necessary information is made available. Yet, information availability does not necessarily equate to responsible action [32,33].

3 THREE CONCEPTIONS OF PRIVACY

The problem of privacy has been a focus of both scholarly and popular attention for decades [29,41]. From a technical perspective, a lot of effort has been made in the design of privacy enhancing technologies (PETs) to address the issue. In their 2010 review, Danezis and Gurses [12] identify three conceptions of privacy that underpin various PETs – confidentiality, control and practice. This classification illustrates how different underlying conceptions of privacy result in systems that attempt to facilitate different kinds of behaviour and allows us to highlight the role of consent mechanisms.

[3] https://www.facebook.com/about/privacy/

[4] https://tinyurl.com/y9t6gdpy; https://tinyurl.com/yb43msya

3.1 Privacy as Confidentiality

The concept of *confidentiality* in the context of information technologies encompasses the individual's right to keep data private and to protect against unauthorized access to information [12]. Properties such as *unlinkability* (the inability to determine whether two objects of information are related), *undetectability* (inability to determine if an object of information exists or not) and *unobservability* (when objects of information are not discernible from one another), are key components for establishing data confidentiality. These properties support the promise of anonymity by disconnecting data from the individual, preventing identification and as a result potentially alleviating concerns for privacy infringement [4]. Anonymity is a difficult proposition as the amount of data about individuals and their practices proliferate and disparate datasets can be combined to enable de-identification [24]. A secondary question remains – anonymity towards whom, the general public, other users or service providers?

3.2 Privacy as Control

The concept of *control* offers a more compromising stance, acknowledging the advantages of data collection provided that it is possible to manage who can access information and in what circumstances [12]. The key to doing so resides "in a combination of a measure of identity control for the user while still providing enough identity data for the service provider to be able to reach and re-identify the user" [18]. As a result, it is the users' responsibility to mediate between the providers of identity management systems and third parties. This approach puts control and decision making in the hands of the user, thus absolving the data collector of responsibility to guard against privacy violations. As Danezis & Gurses point out: "This is of course an illusion, and being in the middle of a sticky situation does not automatically put one in control of anything" [12]. The issues come from the problem with very notion of consent and the common fallacy of the idea that individuals have the power to self-govern.

3.2.1 The problem of consent. Consent mechanisms are crucial for performance of epistemic responsibilities as they are intended to provide the user with the information necessary to make informed decisions [34]. Informed consent is intertwined with responsible action and has become one of the primary gatekeepers of privacy [4]. In reality users are asked to consent prior to use of devices or services by making an informed decision about disclosure of data produced in the future for use by an unknown number of actors for purposes that are mostly impossible to predict. Clearly this is an impossible demand making the mechanism of consent problematic beyond the issue of presenting complex information to users in a simpler form [8,20,39]. Worse, interaction online typically includes both explicit and implied consent mechanisms making the problem even more difficult to unravel [4]. As a result many users feel helpless in the face of data harvesting by digital services [2, 31].

3.2.2 The Fallacy of Self-Governance. The concept of control over personal data is based on the idea that the user is able to evaluate the compromise between privacy concerns and the benefits of achieving a goal from a cumulative and holistic perspective [34]. Yet the boundaries of who is allowed to know what must be continuously negotiated with the ever growing body of entities collecting and processing personal data. People have little time for privacy self-management, even if all the knowledge required to do so is made readily available [27]. Regardless of the users' degree of intent in protecting their privacy, the sheer complexity of understanding and practicing privacy self-management is often too monumental a task to bear [4]. Achieving the goal of effective privacy practice is unlikely, in particular because clearly identifying the compromises actually being made is not possible.

3.3 Privacy as Practice

Privacy as practice is a familiar reframing of privacy to HCI scholars [5,19,29,31,36,38]. In this view, managing privacy in everyday life requires an understanding of social norms, values, and expectations as these are enacted in socio-technical systems in practice. The idea of privacy as practice is harder to systematically implement in digital systems. However, there are several implementations of interest. For example Facebook's implementation of the ability to see what an individual profile looks like to other users is a version of a privacy mirror – a socio-technical design framework proposed by Nguyen & Mynatt [26] in order to address privacy issues present in ubiquitous computing. The authors argue that such a mirror can assist users in understanding a socio-technical system and reflecting on their current practices helping them assess if changes are needed.

As the number of devices and services proliferate, user data management evolves to accommodate these as part of everyday relational practices. The increasing complexity of data sharing and management practices precludes significant attention paid to any one service, privacy policy or end user license agreement [17]. Attending to practice allows us to consider what current digital systems expect the users to do, how users understand these expectations and whether these are

achievable. By focusing on Facebook use in practice, we explore how users think about and perform responsibilities of data management. We take this as a basis for our study and explore how notions of control and confidentiality frame and shape the way participants understand their interactions with Facebook.

4 METHODS

We developed a mixed method framework based on the gamestorming [16] approach as a foundation for engaging with existing Facebook privacy mirror implementations [26]. We used scenario building [23] to surface user privacy practices supplemented by a means-end approach [30] and laddering [28] to afford further elaboration. We used grounded theory inspired mechanisms as a systematic analytical framework for iterative open and thematic coding of our data throughout the study [35].

Gamestorming approach. Gamestorming facilitates activities that enable participants to create representations of their practices, through physically mapping a particular process and then eliciting values in order to experiment with ways to address the emerging challenges [16]. The method provides participants with a goal and a sense of direction while simultaneously remaining flexible enough to allow for emerging topics to be explored. In our implementation, participants were confronted with the goal of *mapping their digital practice on Facebook on paper*.

Means-End approach. In essence, the means-end method is used to explore the interconnectedness between the *means* and the *end*. In addition, it assists in revealing how the user assigns value to different criteria of choice, and why some are weighted higher than others [30]. In our case, we were interested in motivations or attitudes that serve as the driving force behind a user's decision to disclose information. Thus we designed the questions of the opening phase of our interviews to explore and challenge the users' perception of the consequences of their data sharing decisions on Facebook.

Scenario building. A systematic way of simulating situations can be achieved through scenario building. Following Meinert we designed our scenarios to be novel, multifaceted, believable, comprehensive and never right or wrong [23]. Our scenarios (Appendix 1) were intended to confront participants with realistic circumstances. Participants were asked to articulate their feelings and how they would act in such conditions.

Laddering approach. Laddering technique begins interviews with questions that frame and then gradually increases the level of abstraction through questions such as "*Why is that important to you?"* in order to investigate beliefs, feelings and goals behind a specific decision [30]. This is especially useful in semi-structured interviews as it "[...] can produce relatively structured knowledge because the interviewer can slowly ''climb the ladder'' … enabling the creation of meaningful mental maps" [28]. We ensured that our questions moved from very specific to more abstract in each part of the interview.

Privacy Mirror. Privacy is an abstract concept and studies of privacy often run into what many have termed the attitude–behaviour gap or the *privacy paradox* [31,34]. Discussions of attitudes and beliefs can be more productive if participants are confronted with the apparent contradictions between their earlier responses and the reality of their practices. We used Facebook's app permissions screen to make real participant's actual disclosure practices towards the end of the interview.

4.1 Interview Design & Sample Description

Our study was designed to disturb, to surprise and to force participants to reflect on their Facebook use practices. The interviews were designed as a three-phase process (Appendix 2). The opening phase used Gamestorming to map Facebook use practices. In phase 2 we asked participants to discuss the scenarios, while continuously referring to their process map. The scenarios were fictional yet plausible and referenced what users have agreed to in Facebook's EULA and ToS. The closing phase used a Privacy Mirror, asking participants to open their Facebook profiles and walk through privacy settings and app permissions. This confronted the interviewees with what data about them connected applications were accessing through Facebook. Throughout we relied on Means-End and Laddering for structuring our interactions. In doing so we created a situation of deep reflection and discovery anchored in the realities of personal data leakage.

We conducted a total of 21 qualitative semi-structured interviews with participants that identified as active Facebook users, accessing the site at least daily. We stratified by age and gender to attain a diverse sample. Previous research suggests gender and age are important factors in perceived privacy risks [17, 40]. Our sample included 10 male and 11 female respondents to ensure gender parity and comparability. Average age of participants was 35.9 (range 18 to 68).

5 FINDINGS

Throughout the study participants consistently expressed a strong sense of personal responsibility for their actions on Facebook at the same time as they professed frustration and a sense of helplessness. Three themes emerged in our analysis: the notion of ideal or aspirational personal data management behaviour,

frustration with others who fail to live up to such behaviour and frustration with the self for the inability to perform as the ideal required. In the sections below we first describe these themes. We then use our data to reframe how common privacy concerns might be more productively understood.

5.1 The Ideal of Personal Data Management

The majority of attempts to support users in managing their personal data make the assumption that users should be empowered to make individual decisions about data disclosure [8,9,12,20]. Fundamentally, this is rooted in the notion of informational self-determination, the idea that individuals are able to make decisions on their own behalf given sufficient information. In effect, this means that provision of information through ToS and EULA makes the users directly responsible for their data disclosure decisions. Research repeatedly shows that many have internalized this responsibility [39,40]. Our participants too expressed the conviction that they ought to be able to "do better" at managing their own data. Throughout the interviews many noted that they needed to make a more active effort in managing data flows and considering how their personal data was presented in different contexts: *"I think you always have to keep in mind how private you are – what you want to share with who" (Interview #7).*

We repeatedly observed that our interviewees saw loss of control over their personal data as their own fault. Many then argued that it was up to them to regain control and to be more informed. For many it was about the: *"[...] responsibility that you choose to take for yourself and your own information" (Interview #4)*. In fact, the only way to behave responsibly with respect to data was through some form of control regardless of whether privacy was actually desirable: *"That is the weird thing. I'm not quite sure I need to be so private, but I want to be in control" (Interview #5).*

Our data suggests that for our participants there was clearly an ideal behaviour for personal data management that they needed to live up to. This involved taking individual responsibility for being informed, reading policies and ToS, making an effort to be aware of changing data disclosure commitments and managing their own data disclosure practices alongside privacy settings with some panache. This was especially evident during the privacy mirror exercise when participants were confronted with the fact that they had not realized how many apps they allowed access to their personal data. When discovering this some were outraged because they thought they should have had a choice about this or at least a reminder. Others immediately acted by restricting access because: *"[...] this was one thing that I wasn't aware of and it is one thing I can take control of." (Interview #5).* In all interviews, however, participants came back to discussing their own responsibilities and evident failures.

Only four interviewees were already aware of Facebook app settings and had previously adjusted these, explaining: *"[...] it comes back to the more I can do to limit the data" (Interview #11).* Throughout the conversation it became clear that our participants internalized the responsibility for their own data. They saw control and forethought as ideal behaviours necessary to achieve proper data management. They also expected their social ties to behave similarly. Here the tone of discussion often turned to moral responsibility for data hygiene of sorts.

5.2 My friends can't manage personal data

In our discussions of Facebook, the relationship between the company and its users often came up as participants noted that the free service simply means a different kind of economic exchange. At the same time, many felt encouraged that their peers were becoming more informed about the terms of engagement with Facebook and the costs of its use: *"[..] people are getting a lot more aware of the fact that we are the product on Facebook, so how much of a product do you want to be?" (Interview #11)*

Nevertheless, *friends'* privacy practices still proved a cause for concern, especially given the implications of the privacy mirror exercise where it became clear that some of the apps have access not only to their own but also their friends' data: *"We all have those friends who are a bit retarded when it comes to social media" (Interview #10).* After all, if they had to live up to tough expectations of control and forethought to manage their data properly, their friends would need to as well or all their efforts would be for naught: *"[...] it is the same as group immunity. [...] 10% do something about it and the other 90% are ruining it for other people because they don't protect their privacy as far as they should" (Interview #10)*. As a result, our participants shared the same expectation of privacy self-management as an inherent notion of informed behaviour and expected both themselves as well as their peers to live up to it. However, despite their expectations and intentions, their practices did not reflect their responsibilities as initially proclaimed.

Many of the participants privacy concerns appeared as contradictory to their behaviour. We argue that this was not because they did not care about protecting their privacy, but because the options that they had for doing so made the costs too great without any real and evident benefit. For instance, one of the participants stated that

he believed in privacy, ethics and morality and did not want his information flowing everywhere. However, when asked if the second scenario could happen to him, he revealed that he used a skin app to enhance the layout of Facebook and then reflected: *"It's really weird with the skin one because I know it's so [...] stupid that I want Facebook to look differently and then I allow people to take my data and give it to somebody else but then again… it makes me happy!" (Interview #1).* The abstractions of privacy, ethics and morality can have less weight when confronted with the realities of pleasure and enjoyment.

For our participants, responsibilities of data management may be individual, but they also understood that data exposure happens collaboratively just as often. They held their friends responsible for proper behaviour in part because it was not just their own actions that could result in exposure. The expectations they placed on themselves and their friends in terms of personal data management were difficult to accomplish. In a classic move of committing a fundamental attribution error, our participants excused or explained away the reasons for why they struggled to satisfy the ideal of responsible data behaviour but remained demanding of their friends.

5.3 Failing to Live Up to Ideal Data Practices

5.3.1 Interrogating consent. Many participants strived to live up to the ideal of the informed user who cares about their data. Yet, despite their efforts, they consistently failed to do so. This was perhaps most apparent when discussing their consent practices as nearly all of our participants confessed that they had never read or understood the privacy policies or end user license agreements for the services they installed and used: *"I'm just clicking 'yes' at the moment, I'm not going through the actual terms and changes so I don't know the consequence of the 'yes'" (Interview #5)*

The participant quoted above is clearly aware that there is a problem with giving consent without knowing the consequences. When looking into the privacy mirror of app permissions on Facebook, it became clear to many participants that there was a big difference between what they were comfortable with and what they had actually agreed to. Consider the following discussion:

"I think it is totally crazy that it needs so many things. I'm thinking, why is it interested in whether I'm in a relationship, work history, status updates, religious beliefs and pictures."

[Notices the large number of pictures the app can access]

"Is that all of my pictures? [...] I think it is crazy! Can you remove it? [...] I did not know that you could see this. Some of them are from long time ago. I have no idea what this one is" (Interview #8).

The example above starkly demonstrates how consent, even when it is explicit and presumably informed is not a meaningful mode of data disclosure control. Facebook offers a lot of post hoc controls so we asked whether participants might be willing to use the newly discovered privacy controls to adjust their preferences after the fact. The few that had tried to manage their privacy through the Facebook settings, explained that it was an extremely cumbersome process. As one participant reflected when managing which apps had access to his personal information: *"What was really annoying was how difficult it was. There is no remove all or start over function. [...] I think they made it difficult on purpose, both to find and to do something about it, it took me about an hour to remove them" (Interview #10).*

To make matters worse, Facebook frequently updates privacy settings, making it increasingly difficult to ensure that user privacy preferences are aligned with their privacy settings at all times: *"I don't like that because it makes me feel like I never know how my profile is. Which also is something that makes me more cautious when I use it because I don't really feel like I really know." (Interview #14).* Despite the motivation to act responsibly, actually doing so appears to be too difficult and time consuming. Facebook controls are so extensive, granular and varied, that it is possible to get lost in the minutia of multiple ways data are collected and used [27]. Our participants were frequently not sure how Facebook collects or utilizes their personal data, though most felt somewhat uncomfortable about it: "Wow… I didn't know that. [I feel] horrified" (Interview #2). Surprisingly, when we asked them whether they saw themselves as informed, most told us they felt they were more informed than average at least until the experience of our interview.

The ideal of informedness drove many to lament the problem but only four told us they wanted to actively learn more and asked for pointers. The rest took refuge in having a plan to do so at some unspecified later date: *"but I am not totally ignorant. I plan to stay more informed. I know some sites where you can read a simplified version of the terms of use agreements" (Interview #5).* This sort of plan in turn seemed to provide participants with a sense of control until we asked them how likely they were to follow through: *"I know... But I don't do. That's the thing. And I'm a bit embarrassed to admit it, because I'm not fine with it. It is almost like you are asking me about my position in the universe. It is actually not that easy to relate to, because it is something you use every day without really thinking that hard about it and you really have to think hard about*

your behaviour in order to be a super user and protect all of your information" (Interview #5)

It is possible to dismiss the quote above as merely a peculiarly self-aware example of privacy paradox. However, here the ability to be a responsible knower is equated to the ability to comprehend one's "*position in the universe*" and is inherently impossible. While having a plan can provide some sense of control, no matter how illusory that control may be, really thinking about how well one can manage one's data is an overwhelming experience. Perhaps, just making plans for becoming informed are efforts to alleviate the stigma associated with not living up to the expectations inherent in the available privacy mechanisms.

5.3.2 Reversing the privacy paradox. Although the response of consternation in the face of the privacy mirror was common, some participants responded in reverse. Some claimed initially they did not care about what happened to their data, but as we got an in-depth look at what they actually did on Facebook, their practices suggested much attention being paid to data practices. For example, one participant explained: *"But I just do not mind it, and maybe something with the way I use Facebook that I in principle do not care what happens" (Interview #4).* Yet, his Facebook profile was set to *friends-only* and he was also quite careful about what kind of content he posted: *"[..] I've done some things from both the phone and on Facebook and changed the privacy settings a couple of times, for what friends and friends of friends have access to" (Interview #4).*

We observed this reversal of privacy paradox several times. Users initially proclaimed that privacy meant little to them, but had typically taken extensive measures to govern their data with care. This suggests that some aspects of being responsible for personal data have been internalized regardless of the attitudes expressed towards data disclosure. At the same time, those that told us they did not care about what happened to their data were far less outraged or disappointed by their privacy mirror experience. In essence, not caring about data disclosure may be a kind of survival mechanism in the face of the sheer impossibility of real control over personal data.

Further highlighting these discrepancies, we found that even though data management is of great concern for all age groups, participants that were more positive about giving access to their personal data as a trade-off in order to access third party content tended to be younger: "*I always sign in with Facebook. [...] Because it is just much faster for me. I mean, I'm very forgetful – I forget so many passwords that I don't even think I remember my Facebook password. My Facebook is always signed in on my computer. So when I click sign in with Facebook, it instantly signs in*." (Interview #6). Yet even those participants that initially emphasized caution tended to use convenience as an explanation for their use of Facebook apps with suspect access permissions.

6 REFRAMING COMMON PRIVACY CONCERNS

Our data demonstrate that staying informed and behaving in a way that would attain the ideal of a responsible individual in a digital environment is impossible. Yet the problems and concerns we have identified are not new. We consider how these concerns might need to be reframed if they are to be addressed via design or policy decisions.

6.1 Users Do Not Read ToS or EULAs

No matter how well the terms of service or end user license agreements are written, displayed or presented, the majority of users ignore them [8,33,39]. They merely represent a hurdle rather than information offered for an informed decision: *"[...] okay, I agree. How bad can it be?" (Interview #7).* There are simply too many of such documents to read and really pay attention to. Besides, with data being leaked in myriad ways, paying attention to terms of service may seem a futile exercise: *"it's just blocking out the pain and knowledge of me sacrificing myself to the gods of the Internet. Like I just I don't see it anymore" (Interview #1).*

Even when participants were interested and willing to read these documents they came away dissatisfied. Despite the effort that Facebook has put into describing their advertisement and other data use practices, when you get down to it, there is really very little actual choice available. Thus our participants found themselves in a predicament, with no options to decline or negotiate the consent if they wanted to use this service. Informed consent is then a false ideal, as consent mechanisms do not help the users, but rather serve as ways to excuse the data collection practice while making the user responsible for decisions of disclosure [27,32,33].

When asking participants to consider methods that would help them provide meaningful consent, intermediaries emerged as a common solution: *"[...] I know there's a website that tries to sum up the EULAs. I think that's what we need. Just so the average person can get a quick overview of what you have the rights to" (Interview #2).* No matter how well presented or well designed, consent mechanisms make assumptions of the user's ability to essentially 'vote with their feet' if they do not like the data policies. This may be true for small-scale apps, but the social costs of quitting Facebook are enormous. Users disagreed with the fact that in accepting Facebook's terms of service they give Facebook the right

to use their personal information without further explicit requests for consent. This was particularly true of the female participants who were significantly concerned with the fact that Facebook has the right to use the images they upload without the need for explicit consent. Some proclaimed that: *"if I have a Facebook account and the terms say that they can use any of my pictures, yeah I wouldn't be able to be on Facebook then" (Interview #7)*

This is currently a part of Facebook's policies, and, depending on the application settings, other companies have access to personal information and images as well. Perceptions of privacy risks and boundaries of what is considered acceptable have become afterthoughts for Facebook as the users, despite threatening to revoke consent, continue to use the platform. The majority of participants accepted that it is their responsibility to become informed and make informed decisions, even though they acknowledge that it is not a feasible task: *"It is just read it and accept it, or accepted that you just accept it" (Interview #18).*

How can we address this issue through design or policy? After all, it seems untenable despite the efforts. We believe that there is value in reframing what is the problem here to address. Clearly this is about how companies in general and Facebook specifically obtain consent for the use of user data. The question is whether it should be the individual user responsibility to think about and manage what they post to Facebook or whether there is a way to distribute the burden of responsibility somehow. What if it was possible to implement distributed responsibility [32] for assessing and addressing data management among friends, groups or even networks? Is there a way for a service such as Facebook to implement a kind of data commons that would relieve the pressure on individuals and enable better and more informed decision making and negotiation about data use overall? This is both a design and policy concern, where instead of doing data usage as usual, data usage and service provision could be negotiated through collective bargaining implementations.

6.2 Hard to Keep Up To Date With Policy Changes

We find that users are unable to accommodate the requirements of what their consent entails. It was also evident that the participants were unable to keep up with the changes implemented in Facebook's ToS and EULA over time: *"[…] they actually increase the access they have to my personal life without me knowing it, as it is difficult for me to know when they change the terms – I don't think they are very good at communicating it and it is very easy for them to 'slip it under'" (Interview #7).* This is a curious situation where Facebook seems to act like one of those frustrating friends on whom you have to rely despite their evident unreliability.

The sense of being overwhelmed by the gravity of data disclosure decisions, in addition to the changes in privacy settings, can lead people to just give up and hope for the best: *"When Apple comes with an update on the phone, it says AGREE or DISAGREE and you have to read this whole disclaimer through - which you don't every time. You just agree and hope that it meets the requirements. You trust them" (Interview #15).* Participants almost wearily trust that Facebook will do what is right, as the time and effort required to remain informed is not a viable option. As a result Facebook users feel helpless because the frequency with which privacy policies change are difficult to keep up with but important to attend to: *"I wasn't asked about all of these things when I signed up back in the day. These are features they have added later on, so maybe it makes sense that they notify me […] that I haven't changed any privacy settings, but they changed their basic premise" (Interview #10).* Occasionally, they do invest time and effort into managing their settings, only to lose it all when privacy settings are reset to unsavoury and too open defaults after updates to the policies: *"It's because Facebook when they make changes they just make default settings so even if you had really good security at one point doesn't mean you have it now" (Interview #14)*

Most users accept that it is their responsibility to be aware of changes and make decisions accordingly and the empirical material demonstrates that this choice is central for their privacy practices. *"I choose not to share everything" (Interview #4)* is a common response throughout the interviews. The general perception being expressed is that it is up to the individual to be cautious about what data they decide to disclose, and the participants argue that they are in control, because they do not write that many status updates. In this Facebook has succeeded in training its users to accept and internalize responsibility for their actions. There are design suggestions that we could make to note that users perhaps need more information or contextual highlights of what has changed and how this affects them. Yet our data illustrates that such suggestions will only serve to create more fatigue. Instead, we call for more thoughtfulness about the kinds of relationships Facebook has with its users and the kinds of expectations these relationships engender.

The notions of brand trust and brand loyalty are common in marketing literature but are rarely discussed in HCI. Yet trust and loyalty are even more important to consider when thinking about the responsibilities involved in managing user data. As users fail the demands on individuals to act responsibly and to make

decisions about data disclosure, their only recourse is to trust the companies with whom they engage and to hope that trust is warranted. Here participants acknowledge the fallacy of self-governance as they articulate their frustration with unrealistic responsibilities of acquiring encyclopaedist knowledge, in order to engage in informed consent [27].

6.3 It is Difficult to be Private

Despite the diversity in participants' answers, the notion of ideal behaviour and discomfort about the failure to live up to it was consistently formulated. However, we noticed an age-related trend where younger respondents relied on Facebook to manage their social logistics across all areas of life to such an extent that the costs of quitting seemed enormous. However, when confronted with the scenarios and potential privacy risks, the female participants expressed more concerns about their personal data than male participants, confirming prior studies [17]. Instead, the youngest male participants expressed their appreciation of the functionalities provided by Facebook and claimed that there is no reason for concerns as long as the users apply some 'common sense' to their behaviour and come to terms with what they want to disclose.

Older participants, in contrast, were far more concerned and careful about managing disparate data flows: *"I actually make a point of keeping my Facebook account as detached from anything, either business or related things" (Interview #11)*. These users were much more likely to have examined and changed their privacy settings primarily in order to manage the range of personal relationships they have on Facebook and to guard against context collapse [19]. We noticed that the degree with which participants identified Facebook as a personal and private space increased with age. Older participants tended to be more conservative about what sort of content they were willing to share. They were also occasionally bewildered by how others in their social networks might disclose information about them. Where younger participants used Facebook for everything from managing schoolwork or professional contacts to posting family photos, older participants often explained that the major benefits for them were staying in contact with their family and distant acquaintances as well as remembering birthdays. The social costs of not using Facebook for older participants were thus much lower and more bearable.

Regardless of differences in age or purpose of use, all participants routinely failed to live up to their own ideals of informed behaviour. In their attempts to enact meaningful self-governance and privacy practices on Facebook, they acknowledged and accepted responsibility for their own data and then failed to manage it.

6.4 Control and Privacy Self-Management

A common theme in our empirical material is that most of our participants did not necessary want to be more private than they were already trying to achieve. As we challenged their behaviours and their decisions, however, they repeatedly argued that they wanted to be in control of how their data are used. It was the lack of visibility of data flows on Facebook that made it difficult to be in control of personal information: *"[..] one thing that is really annoying is that I don't feel like I have any control; I can't figure out when are people able to see what I'm doing. So if I like something and someone else likes it or someone else likes something of mine, can people see it? I have a very hard time figuring that out, it is not very transparent" (Interview 18).*

The more our participants became unnerved when confronted with the privacy mirror, the more they were likely to use the opportunity to restrict app access. Many then talked about the need for control and transparency to decide who gets access to which information. Some even suggested that they would be more inclined to share their personal information, if it was clearly visible where their data were being sent:*"[..] you would be even more inclined to give up data about yourself if there was open honesty between the company and the user" (Interview #18).* Yet more control does not necessarily mean better able to make informed decisions and enact privacy self-management [12]. In the privacy mirror scenario, we see clear examples of users having the option to control but little insight into the effects exercising control may have. After all, what does it mean in real terms that this or that application has "access to my information?"

Terms such as 'trust' and 'honesty' were mentioned repeatedly when describing the relationship with Facebook. Evidently, our participants would like to be able to rely on the fact that trust and honesty are present in their relationship with Facebook but, frustratingly, these are not certain. Expecting the users to participate and live up to data responsibilities, redirects us to the problems introduced by consent mechanisms. We need to ask how meaningful are the controls available to users to manage their engagements with service providers and applications? What are they asked to decide or prevent, really? Our conclusion is that if we are to try and motivate people toward particular privacy-preserving behaviours, we need to be better at explaining not only why these practices are necessary, but also what they achieve in real terms.

7 CONCLUSIONS

Privacy over the years has been unpacked [29] and defined as many things. Recently, Crabtree et al. [11] attempted to "repack privacy" for a networked world, concluding that if we are to consider privacy in mundane practice, the concept dissolves into everyday concerns with relationship management instead. They are not the first to posit that it may be more productive to conceptualize privacy as a relational concept [25,31,36]. As Nedelsky proposed in 1990: "The concept of privacy captures, illusively, important values such as people's capacity to decide for themselves some of the ways they will or will not enter into relationship with others" [25]. Such a conception of privacy captures the very social nature of this construct. After all, what does it mean to enter into a relationship if it is not about gradual process of mutual disclosure from conversation to shared experience? The decision to share, to extend a hand, to be seen and heard, all of these are decisions about whether to enter into a relationship. This is why when unknown entities turn out to know an unexpected amount about us, this feels like such a violation because the fundamental choice of whether or not to enter into a relationship has been taken away.

Berson argues that "data are not taken or given, rather data are achieved" [7] as part of fostering a data culture. Harking back to old organizational studies [15], from the point of view of Facebook maintaining relationships with its users is a way to acquire and maintain data that is a form of capital. Yet sharing, hoarding, using data are both economic and political acts at least from an institutional perspective. Berson [7] conceptualizes data as an interface between the self and the world – an interface that is constantly rediscovered and negotiated. Through data we connect with the world and with each other and as such, decisions about disclosure necessarily have to be situational rather than prospective as most current PETs demand [12].

This processual view of data and privacy management, clarifies that the expectations set up by the current privacy management infrastructures are impossible and that the infrastructures themselves are inadequate to the task. The systems people engage with have taught them to take responsibility for their own data production and users have to a large extent internalized this. Yet the imagined ideal of responsible privacy management remains impossible to achieve. As people are confronted with problems they take refuge in the idea that if only they could have control they could probably manage better even as they realize such control is illusory [12]. Companies and legal systems then develop policies and technologies to provide some form of greater control. The problem is conceptualizing privacy and data as issues of control leads to individuals continually failing in exercising it. Empowering the user to take control of their data merely shifts untenable amounts of responsibility on them for decisions about data disclosure without actually changing the nature of the relationship they have with the providers of their digital services.

Privacy and data, as Nedelsky, Berson and our participants teach us, are about relationships and it is the nature of relationships that we need to consider. The very idea of a 'privacy concern' comes from the post-hoc nature of the realization of violation as a result of our enactments of relationships with the world. The opaqueness of the kind of social sorting into categories that Facebook performs, even if made visible to those users that know how to find these, will always feel like a violation because the choice of imparting such knowledge is part of the decisions we make in whether or not to have a relation with the entities that surround us. This can be interpreted as a loss of control, but that would be too simplistic. The common solution – give control to the user to either reject the categories or to correct them – addresses the wrong reason for the feeling of violation. In constructing technology to deal with the issues of data we need to ask what patterns of relationships among people and between people and the digital environments, the data production and the infrastructures we build do we want to support?

ACKNOWLEDGMENTS

We are indebted to all of our respondents for their generous participation. We thank anonymous reviewers for their constructive feedback.

APPENDICES

Appendix 1 – Interview scenarios

#	Name	Scenario
1	**Log-in with Facebook**	You find an interesting article from a popular online magazine. The website notices that you are using a software to block their ads. As a result the magazine will therefore not let you access the article unless you turn off the ad blocking software. However, you can keep using the software if you log in with your Facebook account.
2	**The 'Free' App**	One of your friends on Facebook sends you a recommendation to try out a free Facebook game. It is a really popular game, and since your friend has sent you a request, you decide to try it out. Later, you find that the company behind has a partnership with an advertising company known for collecting and selling personal data.
3	**Facebook Ad**	You posted a group picture on Facebook of you and your friends having fun at Roskilde festival posing with beers. You later see that the photo has been used in a Facebook ad. Due to the license agreement you can not change this.
4	**Location based service**	In relation to your work you go to a meeting with your colleagues to meet with several employees from one of your clients. The following evening after the meeting, you notice that Facebook suggests adding the client's employees to your friend list regardless of having no common connections.
Privacy mirror		
	Facebook App setting review	*[Ask to see the participants app settings on Facebook (which apps can see what?). In case of none apps, show them the friends app feature]*

Appendix 2 – Interview structure

1. **Outset**	1.1 Have you had experience using Facebook? 1.2 When did you start using Facebook? 1.3 What is the benefit of using Facebook? 1.4 Have you experienced any problems/shortcomings of using Facebook and the available functions?
2. **Anchoring**	2.1 What are your main purposes of using Facebook? 2.2 What characteristics of Facebook help you achieve these purposes? 2.3 Why is each purpose important to you? 2.4 What purposes could be achieved through other means?
3. Behaviour / Practice	3.1 How do you feel about this situation? 3.2 How would you act? 3.3 Could this happen to you?
4. Practices	4.1 How do you feel about the scenarios? 4.2 How could these scenarios be avoided? 4.3 How do you feel about your current practices on Facebook? 4.4 How would you change your practices?
5. Possible Contradictions	5.1 What motivates you to keep using the service? 5.2 What would motivate you to stop using the service? 5.3 What would need to change in order to make you reconsider using the service?
6. Informed behaviour	6.1 Did you consider yourself an informed Facebook user? *(refer to app setting review)* 6.2 Would you consider your methods for staying informed/increasing your informedness sufficient? 6.3 Which tools / abilities would empower you to provide meaningful consent and engage with the service in a more informed behaviour

REFERENCES

1. Alessandro Acquisti and Ralph Gross. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *Privacy Enhancing Technologies*, George Danezis and Philippe Golle (eds.). Springer Heidelberg, 36–58.
2. Mark Andrejevic. 2014. Big Data, Big Questions| The Big Data Divide. *International Journal of Communication* 8, 0.
3. Hajung Aum, Jinkyu Jang, Minji Kim, Taedong Kim, Hyunyoung Kim, and Jinwoo Kim. 2015. The Impact of Self-presentation and Social Expectation in Continuous Usage: Focusing on Recommendation System. In *Proceedings of HCI Korea* (HCIK '15), 371–377.
4. Solon Barocas and Helen Nissenbaum. 2014. Big data's end run around procedural privacy protections. *Communications of the ACM* 57, 11: 31–33. https://doi.org/10.1145/2668897
5. Natalya N. Bazarova, Jessie G. Taft, Yoon Hyung Choi, and Dan Cosley. 2013. Managing Impressions and Relationships on Facebook: Self-Presentational and Relational Concerns Revealed Through the Analysis of Language Style. *Journal of Language and Social Psychology* 32, 2: 121–141.
6. Michael S. Bernstein, Eytan Bakshy, Moira Burke, and Brian Karrer. 2013. Quantifying the invisible audience in social networks. 21. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI 2013).* ACM

7. Josh Berson. 2015. *Computable bodies: instrumented life and the human somatic niche*. Bloomsbury Academic, an imprint of Bloomsbury Publishing Plc, London ; New York.
8. Rainer Böhme and Stefan Köpsell. 2010. Trained to accept?: a field experiment on consent dialogs. In *proceedings of Conference on Human Factors in Computing Systems (CHI 2010).* ACM
9. Jan Camenisch. 2011. Identity management tools for protecting online privacy. In *proceedings of ACM workshop on Digital identity management.* ACM
10. Yoon Hyung Choi and Natalya N Bazarova. 2015. Self-Disclosure Characteristics and Motivations in Social Media: Extending the Functional Model to Multiple Social Network Sites. *Human Communication Research* 41, 4: 480–500.
11. Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking 'Privacy' for a Networked World. *Computer Supported Cooperative Work (CSCW)* 26, 4–6: 453–488.
12. George Danezis and Seda Gürses. 2010. A critical review of 10 years of Privacy Technology. In *Proceedings of Surveillance Cultures: A Global Surveillance Society?*
13. Sauvik Das, Adam Kramer. 2013. Self-Censorship on Facebook. In *proceedings of ICWSM.* AAAI
14. Nicole B. Ellison, Charles Steinfield, and Cliff Lampe. 2007. The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication* 12, 4: 1143–1168.
15. Martha S. Feldman and James G. March. 1981. Information in Organizations as Signal and Symbol. *Administrative Science Quarterly* 26, 2: 171. https://doi.org/10.2307/2392467
16. Dave Gray, Sunni Brown, and James Macanufo. 2010. *Gamestorming: a playbook for innovators, rulebreakers, and changemakers*. O'Reilly
17. Nick Hajli and Xiaolin Lin. 2016. Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics* 133, 1: 111–123.
18. Mireille Hildebrandt and Serge Gutwirth (eds.). 2008. *Profiling the European citizen: cross-disciplinary perspectives*. Springer
19. Bernie Hogan. 2010. The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online. *Bulletin of Science, Technology & Society* 30, 6: 377–386.
20. Luke Hutton and Tristan Henderson. 2017. Beyond the EULA: Improving Consent for Data Mining. In *Transparent Data Mining for Big and Small Data*, Tania Cerquitelli, Daniele Quercia and Frank Pasquale (eds.). Springer 147–167.
21. Cliff Lampe, Donghee Yvette Wohn, Jessica Vitak, Nicole B. Ellison, and Rick Wash. 2011. Student use of Facebook for organizing collaborative classroom activities. *International Journal of Computer-Supported Collaborative Learning* 6, 3: 329–347.
22. Aleecia McDonald and Lorie Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society.* 4, 3: 540–565.
23. Sascha Meinert. *Field manual - Scenario building*. ETUI, Institute for Prospective Analyses (IPA), Berlin.
24. Arvind Narayanan and Ed Felten. 2014. No silver bullet: De-identification still doesn't work. *White Paper*.
25. Jennifer Nedelsky. 1990. Law, Boundaries, and the Bounded Self. *Representations*, 30: 162–189.
26. David H. Nguyen and Elizabeth D. Mynatt. 2002. *Privacy mirrors: Understanding and shaping socio-technical ubiquitous computing systems.* Technical Report. Georgia Institute of Technology.
27. Jonathan A Obar. 2015. Big Data and *The Phantom Public* : Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society* 2, 2: 205395171560887.
28. Peiyu Pai and David C. Arnott. 2013. User adoption of social networking sites: Eliciting uses and gratifications through a means–end approach. *Computers in Human Behaviour* 29, 3: 1039–1053.
29. Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of Conference on Human Factors in Computing Systems (CHI 2003).* ACM
30. Thomas J Reynolds, Jerry C Olson. 2001. *Understanding consumer decision making: the means-end approach to marketing and advertising strategy*. L. Erlbaum Associates, Mahwah, N.J.
31. Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: perceptions of privacy and mobile app use. In *Proceedings of Conference on Human Factors in Computing Systems (CHI 2014)*
32. Judith Simon. 2015. Distributed Epistemic Responsibility in a Hyperconnected Era. In *The Onlife Manifesto*, Luciano Floridi (ed.). Springer International Publishing, 145–159.
33. Judith Simon and Irina Shklovski. 2015. Lessening the Burden of Individualized Responsibility in Socio-Technical World. Retrieved from https://doi.org/10.3390/isis-summit-vienna-2015-T3.3005
34. Daniel J. Solove. 2013. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* 126: 1880–1903.
35. Bernd Stottok, Martin Bergaus, and Andrea Gorra. 2011. Colour Coding: An Alternative to Analyse Empirical Data via Grounded Theory. In *proceedings of 10th European Conference on Research Methodology for Business and Management Studies.* France
36. Emily Troshynski, Charlotte Lee, and Paul Dourish. 2008. Accountabilities of presence: reframing location-based systems. In *Proceedings of Conference on Human Factors in Computing Systems (CHI 2008).* ACM
37. Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, useful, scary, creepy: perceptions of online behavioural advertising. In *Proceedings of SOUPS 2012.*
38. Janet Vertesi et al. 2016. Data Narratives: Uncovering tensions in personal data management. In *proceedings of CSCW 2016*. ACM
39. T. Franklin Waddell, Joshua R. Auriemma, and S. Shyam Sundar. 2016. Make it Simple, or Force Users to Read?: Paraphrased Design Improves Comprehension of End User License Agreements. In *Proceedings of Conference on Human Factors in Computing Systems (CHI 2016).* ACM
40. Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviours Among United States Internet Users. In *proceedings of Symposium On Usable Privacy and Security (SOUPS 2015)*, 309–325.