Users' Responses to Privacy Issues with the Connected Information Ecologies Created by Fitness Trackers

Zablon Pingo[1] and Bhuva Narayan

University of Technology Sydney, Australia
{zablon.pingo, bhuva.narayan}@uts.edu.au

Abstract. With increased innovation and adoption of digital technologies in our everyday life for various purposes, media, privacy experts, advocates, scholars and researchers have noted and raised privacy and security concerns associated with the misuse of personal information from digital technologies. These technologies enable collection, processing and re-puposing of personal information for various purposes by commercial and interested entities.This paper presents a privacy awareness perspective in an attempt to understand how people respond to privacy concerns while using activity tracking devices and applications, loyalty cards and related data sharing within various information ecologies. The research used a constructivist paradigm; we interviewed twenty-one users of activity trackers and loyalty cards to understand their privacy practices. Results show that privacy is a flexible concept which is a result of users' negotiation between the benefits and the harms of disclosing personal information.

Keywords: Activity trackers, fitness trackers, privacy, privacy awareness, informational privacy, contextual integrity.

1 Introduction

Digital services and infrastructure are increasingly beneficial to consumers everyday life; however, scholars, researchers, experts and journalists have raised significant privacy concerns across the digital technologies [1-3], which threaten to deprive consumer benefits through profiling, surveillance [4-7] dataveillance [8], personality profiling for targeted marketing and other purposes [9]. The consequences of these practices are associated with bias in information access [10], social and economic inequality, self-harm, financial loss, hidden influence and manipulation, price discrimination, and censorship among others[6, 11]. These growing privacy concerns and risks arise from service providers' misuse of data, processing, and repurposing from multiple sources not limited to search engines, social media, loyalty systems, and consumer Internet-connected devices like fitness trackers, among other digital technologies [12, 13]. The ever-increasing privacy risks require users of information technologies to have some level of awareness and privacy protection strategies.

To understand and protect consumers' privacy on digital technologies, most studies take legal and information systems approaches[14, 15] but not much is known from users' experiences, perceptions and responses towards the efforts of managing information flows in activity trackers. Privacy protection in the current information age depend on a range of mechanisms including: improving security of the technologies through securing the systems, public policy and individuals awareness to the privacy concerns to determine the risks of sharing such information openly online or to organisations without a good understanding of the surrounding practices[13]. Privacy awareness is essential to compliment the existing mechanisms of ensuring individuals have some understanding and recognition of how information is tracked, used and potentially misused in online environments, for individuals to take appropriate measures to protect themselves [16]; individuals need to evaluate their information sharing practices, and understand how the data they produce is used, shared and loses its private nature[17].

[1] Corresponding author

While most of the privacy studies evaluate technical aspects of privacy and security of the fitness devices and the applications [15, 18, 19], this study provides a qualitative perspective of users' everyday privacy practices while using devices and related synergies created around them. This paper adds to the privacy literature by providing accounts of how consumers respond to privacy issues raised in popular everyday technologies; in this case fitness trackers, and loyalty card systems which have created complex information ecologies that collect and open up personal information to third party organisations [20]. Information ecologies in this context refers to the interconnected nature of socially produced data as a result of human activities popularly known as "social big data". For example, Coles Supermarkets in Australia have introduced synergies where consumers can link their loyalty cards with fitness tracking devices, and since the company also sells insurance, it has implications for potential device and data linkages[21].

The study attempts to answer the research question: How do people manage privacy in regard to the connected information ecologies created through the use of activity trackers and loyalty cards systems in everyday life? What strategies do people deploy to protect their privacy when using fitness trackers and the information ecologies around them?

2 Research Context

In the current data-driven economies there are apparent negative impact to individuals occasioned by use of personal information by data brokers, without the subject's knowledge or understanding, consequently violating individuals' rights to privacy[6, 22]. Informational privacy has become important due to the increased exposures and associated risks in digital technologies[12, 13, 23] making it an important aspect worth exploring from multiple perspectives including understanding how people respond to privacy concerns. Scholars have explained people's privacy attitudes, perceptions and behaviours with findings indicating a discrepancy between behaviour and perception, which is popularly referred to as privacy paradox [24].

While most privacy research takes legal and information system approaches, this research presents a human-centred perspective of users' privacy management practices through consumers' experiences and practices in digital technologies. It is important to understand how individuals take appropriate measures to protect their privacy rather than relying on normative practices to privacy protections. Thus privacy awareness is presented here not as a way of "setting rules and enforcing them"[25] but as a way of exploring how users understand and use a series of strategies to protect informational privacy in various digital technologies.

3 Privacy in the Context of Interconnected Information Ecologies

With the increased use of Internet-connected devices, privacy has become an important concept debated and regulated across the world through national and international laws. Hence, understanding users' privacy concerns and awareness in the current information age, where activity trackers and loyalty systems are ubiquitous, is important. This is because these digital technologies increasingly require information subjects and recipients to manage informational privacy in individual and organisational contexts. The technologies enhance connection and production of data and also enable information to get out of the envisaged contexts and boundaries, which can be considered as a breach of privacy [26].

Generally, data subjects or users of the technologies are required to determine appropriateness of information to be shared, while the recipients or organisations or data holders are expected to use the information in accordance with their intended purposes. The privacy as contextual integrity framework provides an important lens to evaluate how different parties manage this information flow. Since privacy is a socially negotiated and constructed phenomena in social processes, Nissenbaum argues that individuals should understand and have the means to manage informational privacy within their social and economic contexts [26]. Nissenbaum [27] further posits that most spheres of life are guided by "norms of information flow" in the sense that not "anything goes." To ensure privacy of individuals is protected, personal

information within information ecologies should flow appropriately in accordance to [these] information norms"[28].

3.1 Personal Activity Trackers, Lifelogging, and Related Data Practices

Consumers use a variety of devices to capture and archive everyday life activities in a process referred to as lifelogging [29]. The self-tracking/lifelogging devices dominating the current consumer market are personal activity trackers or fitness tracking devices and applications. The activity trackers or fitness trackers are electronic devices characterised by the following features: worn on users' body, use accelerometer, altimeters, or sensors to track a wearer's movements and biometric, and uploads activity data to online applications [30].

The devices and applications are used for the purposes of keeping track of fitness and health through monitoring body activities and workouts such as sleep patterns, daily steps, floors climbed, intense activities (like swimming, cycling, resting time), calculating fitness-related measures, calories burned, quality of sleep, cardiovascular workouts etc.[15]. These wearable devices collect various kinds of information including data on bodily functions and physical activities (sport activities, sexual activity, travel), medical symptoms (headache, pain, allergies), spatial data (location, time, what you see) consumption data (alcohol, nicotine, caffeine, water, drug, etc.), mental health data (mood, stress, alertness), and physiological statistics [31].

Additionally, during the device set-up, users provide demographics including: gender, age, identity (photo, name, biometric data), and relational data (email, phone number). Once one starts to use the devices, personal health information or health activity data is collected, including heart rate, body mass index or BMI, weight, sleep data, calories burned, GPS locational data, dietary logs, etc. [15, 32]. The gadgets also synchronise wirelessly with other devices to provide additional information such as: text notification, calls, caller ID, and music control, and they are also compatible with third party applications and other mobile gadgets [15].

Researchers note that these self-monitoring practices are motivated by the need for recording things for one's own use and for memory purposes [33] and the practices are now commonly referred as quantified-self for the purposes of monitoring body fitness or health [34, 35]. Lupton [35] notes that while the users purchase the devices for personal use, the data is managed on proprietary platforms or databases which are involved in the data politics [36, 37]. This raises fundamental concerns and questions of how to maintain users' data privacy [35]. The data produced by these devices have become of interest in the current big data discussions and data politics, given the new business synergies created around them such as the example of Coles retail stores and insurance companies in Australia [21, 35, 38]. These self-tracking technologies and practices have risks as well as benefits given their pervasive nature to capture contextual data in a continuous manner and the use the data for health research and management purposes[35, 39, 40]. The expanding body of data capturing presents a wealth of resources for data analytics, especially behaviour analysis for targeted marketing among others opportunities[6]. Lupton further notes the positive side of the use of data captured from these sensor equipped devices can potentially offer solutions to improve efficiency in safety, wealth generation and resource management in various sectors especially health, education, environment [36] and development of smart cities.

Whilst this data can be beneficial to users, the lifelogged information is sensitive [33], and hence prone to privacy breaches [15] and misuse beyond the users' knowledge. Researchers argue that digital technologies are increasingly used as a monitoring tool and as disciplinary tools to regulate human behaviour by exerting power over individuals through collection of data and profiling [41]. For example, the wearable devices can be used to investigate user activities, travel and driving behaviours of individual's and predict individual lifestyle characteristics [42] and so on.

3.2 Privacy and Security Concerns in Activity Trackers

Neff and Nafus [37] note that privacy and security challenges in activity tracking devices are technical ones; others are demonstrating this through compromising selected popular consumer activity trackers [43,

44]. These products also provide a range of features for users to control their information sharing with other applications like social networks [45] and the ability to share data with other people and to third parties for personalised programs [15].

Additionally, the Symantec security experts note that most trackers can easily be turned into surveillance tools by unauthorised third parties given the ability to track the location of people [31, 37]. A study of communication between activity tracker and online web servers also identified critical vulnerabilities, which can compromise users' privacy and security [44, 46]. Similar experiments confirmed the security vulnerability of the popular fitness trackers (Garmin, Fitbit, Xiaomi, Misfit, Polar) possible illegal access to device servers and manipulation of the data [18]. In an experimental study on Fitbit and Lose it! applications, researchers found users can permit third party apps to access data from their devices including calendars, camera, contacts, locations, microphone, phone, sensors, SMS, storage) and other metadata which is unknown to the users of the applications [15].

The fact is that service providers hold a great amount of data about people around the world, including medical devices connected to the Internet, with an ability to transmit data from data subjects. For example, pacemakers that capture and send cardiac rhythmic data to manufacturers' data warehouse and doctors for patient monitoring purposes, while the data producers/data subjects have limited access to their data, demonstrates a lack of control by the individuals [47]. This was demonstrated by Hugo Campos, a user of medical device- implantable cardioverter-defibrillator (ICD) who tracked his body fitness activities using an activity tracker, but had to file a court case to compel the ICD manufacturer to give him access to his own data; he was the data subject but did not have access to it [48]. Campos' [48] experience of denial to access or lack of control to the data produced from his heart monitoring while doctors had full unrestricted access to the information demonstrate data holders' immense power over the restricting access to these form of data although the data is about users' own body [48]. This incident forced Campos to sue the manufacturer of the devices after being informed that the data generated from ICD was "proprietary data"[49]. This example indicates how the data produced from IoT devices are implicated in data politics and legal battles over the ownership of data, which openly indicates that the data belongs to third parties and not to the device users or the data subjects [48]. Fixing the security and privacy issues raised in the big data and Internet of Things era is complex, and needs both technical solutions, legal alignments with the challenges, and users' awareness [15, 45, 50].

3.3 Third Party and Other Activity Trackers

Fitness tracking devices and apps also have third party applications which users can connect their devices or data to for other additional services [15]. For example, a user of Fitbit application or device can allow or deny access to Fitbit data access by the third party who also have their own privacy policies. Some of the data, which can be accessed include: sleep data, food, water logs, activity and exercise, and weight, which users may knowingly or unknowingly understand what terms are tied to such linking of the data and what third parties put the data into which use. The applications include Lose it! and Strava [15]. The applications collect data from phones and fitness trackers and allow users to share the routines with friends and followers, on social media, which sometimes may pose security risks to the users due to the ability to locate individual routine or physical location. In addition the fitness devices, applications can be linked to other applications and systems where consumers are presented with incentives to share personal information in-exchange for services or reduced insurance premiums [21, 51], as presented in Figure 1.

4 Research Design

The research design was guided by the objectives of the study to understand users of activity trackers and loyalty card systems and privacy perceptions, and how they manage personal information in the applications. Thus in this study we were interested in understanding users privacy awareness and protection practices, with the increasing use of the devices and application for self- monitoring, health monitoring and sharing of the data for other services.

For participants to be eligible to participate in this study, they fulfilled the following criteria: were 18 years or older and must have been using at least one of the activity tracking devices and using a membership card

or loyalty card. The participants were invited to participate in the study through social media messages, university listserves, bulletin-board flyers and through word of mouth. The participants were between the age of 19 to 52 years old with 12 females and 9 males. All the participants were actively using a variety of fitness tracking devices and popular loyalty cards within Australia as referred in the Table 1.

The research used a qualitative approach through face-to-face interviews to get insights on how participants' experience and manage their information and data privacy according to their preferences. The use of semi-structured interviews offered a flexible opportunity for the interviewees to answer the questions [52]. Twenty-one participants from Sydney Australia were interviewed between November 2017 and December 2017 in forty-five to one-hour-long interviews. The names of the participants have been anonymised through the use of pseudonyms to ensure the privacy of the participants.

Table 1: Participant Demographics

Participants (Pseudonyms)	Gender		Age Range	Activity Tracker	Loyalty card
	M	F		Type	
Kelly		X	30-39	Fitbit	X
Vera		X	20-29	Fitbit	X
Marcello	X		20-29	Garmin	X
Deepak	X		20-29	Garmin	X
John	X		40-49	Fitbit	X
Elaine		X	20-29	Fitbit	X
Molly		X	30-39	Fitbit HR2	X
Dolly		X	20-29	Fitbit	X
Janet		X	30-39	Fitbit	X
Sue		X	20-29	Fitbit, Apple watch	X
Harry	X		20-29	Fitbit	X
Teresa		X	40-49	Fitbit	X
Michael	X		40-49	Fitbit	X
Evelyn		X	40-49	Fitbit	X
Ivan			40-49	Fitbit	X
Lillian		X	20-29	Garmin, Fitbit	X
Pauline		X	40-49	Garmin	X
Julie		X	40-49	Fitbit	X
Daniels	X		10-19	Xiaomi, Apple watch	X
Joe	X		20-29	Fitbit, apple watch	X
Andrew	X		50-59	TomTom	X

The interviews were audio-recorded, transcribed for analysis and later coded in NVivo for thematic analysis. The NVivo was used to collate related themes and for finding patterns within the data to facilitate the analysis [53]. Although the study was informed by the contextual integrity theory of privacy [26] we used thematic analysis to identify all the patterns emerging from the interview data. The interviews were guided by the overarching questions of how people manage personal information flows across the synergies created through activity trackers, users' privacy concerns, and behaviour toward affordances that link data across organisations or third parties. Finally the participants were also asked about the use of privacy settings within the activity tracking application and their awareness of the privacy policies of the respective services.

5 Findings and Discussion

The data analysis identified participants' informational privacy preferences and management practices in their everyday-use of the activity trackers and possible connections with the loyalty cards and to other additional applications. Various themes emerged during the analysis process, including: appropriateness of

information shared in particular platforms, information avoidance and privacy policies, managing data sharing practices including locational data, which are all presented below.

5.1 A Negotiating Attitude Toward Determining Information Sharing

Normative notions of privacy management require users of digital technologies to assess the risks of providing or disclosing personal information on online platforms or to organisations versus concealing the information. Since the personal information collected through these devices and applications represent a person's identity and everyday-life activities, misuse of this information might have possible privacy implications.

Such privacy concerns compel users to take precautionary measures to limit the amount of information when signing-up or sharing across applications. The interviewees were asked about their responses to linking fitness data with other applications or services and were presented with scenarios such as the existing retail store program in Figure 1, which allows consumers to link loyalty cards systems, activity trackers and insurance providers in exchange for benefits. The program provides a means for users of the devices to link the fitness tracker data and loyalty cards and share the data to an insurance provider in exchange for points or reduced insurance premiums.

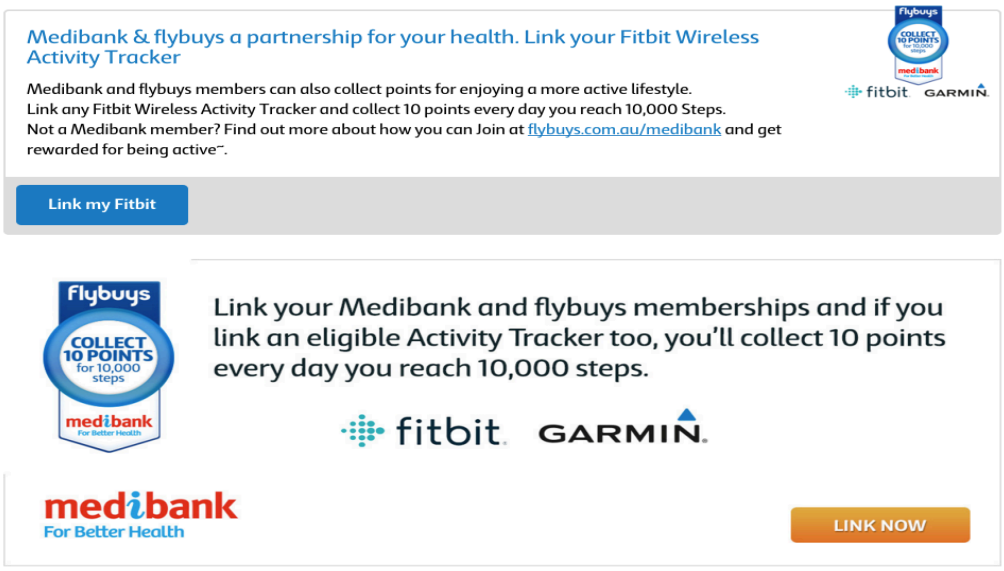

Figure. 1 Flybys loyalty system connects with activity tracker and insurance provider [21]

While the majority of participants considered the information in fitness trackers as sensitive and uncomfortable to share due to privacy concerns, twenty of the participants were also willing to share or link the devices in return for tangible benefits. This can be attributed to consumers' motivation to satisfy their immediate needs while considering privacy as a distant concern ("why would anyone be interested in me") with possible minimal impact ("I have nothing to hide") compared to the benefits derived from the use of the technologies or making such connections that allows organisations to link and use the derived data.

The finding corroborates prior research, which indicated that users of various digital technologies are willing to share most form of data for instant monetary gratification [54, 55]. These responses are partly associated with peoples' perception of this information as something that only exists in a virtual world that is less likely to impact on their real life; this may have an influence on consumers' behaviours towards making such trade-off decisions [56]. For example, although our research participant Julie was concerned about how the fitness data might be used against her due to concerns about her health status, she was willing to make such a trade-off for instant monetary in exchange for sharing fitness information:

"If actually sharing my information was going reduce my premiums I absolutely do it, but I don't know that would be the case. It might actually take my information and go while you're overweight. Therefore we're going to increase your premiums. I think for me the insurance companies will be happy that someone who's is overweight as me with my family history both my parents are overweight as well that I'm actually exercising as much as I am"

Due to perceived economic effects, individuals are likely to share data with such connected synergies by making a quick cost-benefits analysis; as Julie further explained:

"I don't know I mean it's a tricky situation because in one sense I'm really healthy because I'm exercising a lot. But honestly at the moment I am so poor maybe I would, just because if reduces my premiums then I would."

Other participants also indicated similar sentiments of readiness to link their loyalty cards and fitness data for monetary benefits:

"I am open to doing that, because it reduces cost, for minimal effort on my part. Reduced privacy for at least some money."

While participants considered the information from their fitness trackers as sensitive health data and uncomfortable to share, only one participant had extreme concerns towards the sharing and connecting of fitness trackers and loyalty cards with insurance companies, or participating in such reward schemes. For example, one respondent said:

"I'm very wary of giving more information to my insurance and I wouldn't want to do is. it can quickly be used against me or use for the wrong purpose. And once it's given that I don't have any control of how this will be used whatever is a good intent. I guess I am somehow very conservative person and I don't want my insurance to know what I'm. Why I'm Running. How many times I'm running. How is my heartbeat going, maybe it's my conspiracy theory thing but yeah I'll think it could easily then be used for reviewing maybe terms and conditions of my insurance and I wouldn't want that."

Amongst all the participants only one participant was unwilling to share or link the devices and share personal data from the activity tracker for any benefits. The findings demonstrate the vulnerability of users towards the trade-off of health/personal data for instant benefits while ignoring their privacy concerns arising from the use of the data.

The activity tracker applications also provide a means for users to share their fitness data on social media like Twitter, Facebook and other third party applications. The majority of participants indicated a lack of interest in sharing their fitness data on social media with the exception of a few who indicated that they had posted the fitness data on social media to share their achievement while training for some up coming marathon events.

The willingness of consumers to make such trade-offs in sharing information across contextual boundaries and also to make a considered and rationalised decision when deciding to share their data while knowing possible future risks is in line with findings from earlier research [54] which indicated that people have adopted an "it depends attitude" when it comes to sharing personal information for economic benefits, although privacy experts and researchers raise the possibility of misuse under such trade-offs because users hardly have time to understand all the terms and conditions of such services.

5.2 Controlling Locational Data in Activity Tracking Applications

For the Internet-connected and GPS-enabled activity tracker devices, it is difficult for consumers to control locational data due to covert and technical transmissions of locational data. Also when users set-up the activity trackers they provide personal information, which includes name of the place, users personal

information (name, e-mail address, age and any characteristic that is unique to a person) and locational information: spatial (coordinates) and also temporal information (non-real time and real time)[57]. The locational information disclosure in the activity tracker applications is both technical and voluntarily shared with third parties and service providers. For example, the fitness tracker applications permit users to share locational information in the device applications [18] with other users or on social media, thus individuals have some form of control to decide whether to disclose, or not use the locational feature. One participant indicated that they have connected the fitness application to another third party application (Strava) to map distance and route used etc.; however, due to security concerns about people being able to locate her home, she disconnected and deleted the application:

> *"I'm very concerned with some applications they know already where I am through my mobile phone not just Fitbit. Yeah there was this app- Strava I used, but I stopped because it knows my location like home. So if I'm doing a run it will know that I'm always stopping in one area and Ill know that that's my base and therefore that was my home. So I stopped using that."*

To control the flow of locational information, participants indicated continual effort and attempts to limit access by deactivating locational features on their smartphones or applications and avoiding using the location features in fitness application or avoiding using automatic uploads of the data to their social media platforms like Facebook or Twitter. For example, Pauline explained why and how she limits access to location information for privacy reasons:

> *"I want to limit my exposure of my personal information as much as possible. I don't use my location on my phone or fitness trackers because I don't want people out there to know where I'm located. So only when I'm desperate and I need to go somewhere, I use Google Maps, then I put my location on and then as soon as I finish up takeoff my location."*

Teresa also explained that she always denies access to location while using smartphone applications, and only activates location service in the applications when necessary:

> *"I don't like sharing my location for every application. Just [that] I have a bad feeling about being monitored, about people knowing exactly where I am and I just it's just does not sit comfortably with me."*

Majority of the participants were highly concerned about locational privacy concerns especially in disclosing their home addresses and their real-time location for security reasons. Most of the participants indicated they enabled the location functionality when using some applications on their smartphones applications. While protection of location privacy takes multiple perspectives, the findings indicate users of the applications actively deploy necessary measures within their means to maintain their locational privacy by controlling the locational information sharing in devices and applications.

5.3 Complexity in Managing Personal Data

Social media applications provide privacy settings to limit access to personal information by an unintended audience or unauthorised individuals. The activity tracker devices and applications equally provide privacy settings to enable users to limit the type of information that should be accessible to other fitness applications.

However, in this study, the users expressed their lack of complete control over the personal data in devices since they are Internet-connected devices and due to the complexity of the interconnected technologies. The participants pointed out that while the fitness applications provide new opportunities for personal use, they equally pose unknown risks to users. For example, one participant reflected on the challenges of understanding how to balance between the "new opportunities of using the digital technologies and managing the privacy risks". The participants pointed out:

> *"...given the options in a very clear simple way to manage my own privacy then I would really like to have that because at the moment it's quite cryptic sometimes and it's all hidden somewhere*

and it's like if we're looking at one app but then we don't know where and how far it's linked to all the different devices and all. So it's not just the app it's the devices and it's other people's devices and then it's always linking a lot of different things thinking other people's devices my devices my time, my location. So how much I can control that I don't know because it's so new it might also with new opportunities or new threats as well that we may not be aware of especially malicious ones."

The fitness tracker applications provide privacy settings to enable users to control personal demographics (birthday, height, weight) and statistical information on calorie intake and calories burned, sleep, distance walked, steps taken, floors climbed etc., and post graphs and posts within the application and social media platforms. The application allows users to customise the settings with three options to make the personal information private, public or share it with friends within the networks or to social networking sites.

In many of these fitness applications, users can form groups in the application and share fitness information and make comments on other users' profiles just like on social media or social networking sites. None of the participants indicated having used or customised the privacy settings. This could be attributed to most participants having no interest in sharing the data in their respective social media even though it is possible to avail opportunities to share the data/information. The privacy settings feature requires effort and some form of privacy literacy to understand how they function, in order to meaningfully use them to safeguard the informational privacy of oneself and others.

5.4 Information Avoidance, Privacy Policies and Privacy Management

All the twenty-one participants did not read the privacy policies before using or signing up for the fitness and loyalty cards systems. While the privacy policies are presented as main tools to negotiate and inform users of digital technologies on how the information is collected, processed and used by the service providers, participants indicated they never read them because of the information overload they present. The participants explained:

*"I kind of start reading that and then; I think nobody actually reads all of that, everyone just clicks. I agree, and that's all. It's too much information and it's boring." (*Elaine)

"It's a bit time consuming and no one can actually read it. If you get privacy statement, you just click agree and move on to the next step" (Deepak)

Information behaviour researchers explain that people deployed information avoidance as a coping mechanism to deal with cognitive dissonance and information overload [58]. Thus, with the negotiated nature of privacy, and on account of the legalese presented in privacy policies, a kind of cognitive dissonance is triggered, compelling users to take a passive role in consuming the technology without making an effort to understand the consequences of such behaviour for their informational privacy. The participants' behaviour reflects lack self-determination in privacy negotiation. For example, Julie said:

"I am lazy with privacy policies, because it's too long and I think that makes me very loose with my privacy."

Similarly, other participants noted that privacy policies present constraints due to a lack of choices, saying that the conditions were rigid in the way consumers have to agree to the terms as presented. Teresa explained that she superficially glances at the privacy policies and finally agrees anyway, since the alternative is to forgo the use of the product or application altogether, which is not an option at that particular moment:

"*I read them in a very superficial way and sometimes I don't read because I figured that if you want to use the devices or application you have to agree with the policy. If you don't agree with the policy don't use the device use some other mechanism."* (Teresa)

> *"I know everyone should read that, but...it's just like maybe I don't really care if they're going to share my names with somebody, or my email, or something like that because it's not too personal information. If it would be more serious information like my bank account, or something like that, yeah, I would definitely read all of that. But because it's only my name, date of birth and how much I weigh, it's not that serious."* (Vera)

The continual avoidance to use privacy policies calls for new ways to enhance their use either through active measures such as stringent data protection regulation by privacy regulators to compel service providers to address the complexities, and for the users to equally negotiate or understand the synergies around the data collected from the devices and applications. For example, researchers and privacy advocates have increasingly proposed improvements to the mode of presentation and transparency through simplification of the language and fonts and the provision of choices of opting-in or opting-out that clearly indicate the how the collection, processing, transferring or sharing of personal information is done [59].

While privacy is presumed as a fundamental right, users of digital technologies have limited control or lack the means to exercise that right due to the limited options. Additionally, people give consent to the terms of service without reading them, which indicates vulnerability due to a lack of understanding of how the data is used by third parties or service providers. To address the constraints in the privacy policies, new mechanisms have emerged to advocate for improvement of privacy policies and terms of services with organisations and researchers dedicating themselves to analysing technological corporations privacy policies which provide consumer-friendly privacy policies [60] in an effort to support general public awareness. These approaches are deliberate attempts to enhance transparency and openness in protecting users' information privacy and also enhance privacy awareness among the users. This may foster usability of the policies rather than having them serve purely legal functions, negotiation and informing tools of how the data is collected, processed and used, in a clear, simple-to-understand language.

6 Conclusion

This study examined users of activity trackers and loyalty cards to understand their privacy awareness and use and sharing of data. Past research on mobile-device fitness applications suggest the use of the "Inform, Alert, Mitigate" method to enhance users' privacy awareness in applications to ensure users have control on how the information is collected and used [61]. Although this method is effective in giving some degree of privacy and data control to users, the business synergies created around data may by-pass these controls.

The study findings show individuals use a variety of methods in an attempt to protect their data and locational privacy; however, the practices are not consistent due to users' attitudes toward the trade-off of data for benefits. While the study findings indicate user awareness of privacy concerns associated with sharing information in digital technologies, they also point to a vulnerability due to the willingness to share data in exchange for benefits without understanding the terms of services. The readiness to share personal information with third parties and service providers without reading or understanding the terms of service call for more transparency in the way service providers inform how they collect, process, transfer and use personal information. This will ensure the usability of the information in a beneficial way by users and also enhance consumers' trust in service providers and related entities.

Additionally, the continued reluctance by users to read privacy policies indicates a vulnerability for users, and hence service providers need to be open on how they preserve the contextual integrity of the data they collect intentionally or inadvertently, and how they handle the information flows, with the protection of consumers in mind.

As indicated in the literature, researchers have raised privacy and security concerns related to activity trackers, and therefore it is important for users to understand the vulnerabilities they are exposed to while using these applications and devices. Users' knowledge, skills and awareness of privacy issues is integral to the contextual integrity of the information and data that and service providers collect. Therefore, they

should also take the responsibility to educate users and provide an enabling environment for users to manage their personal information and privacy according to their expectations.

References

1. Solove, D.J., Schwartz, P.M.: Consumer privacy and data protection. Wolters Kluwer, New York (2014)
2. Christl, W., Kopp, K., Riechert, P.U.: Corporate surveillance in everydaylife, Crackedlabs (2017)
3. Rosenblat, A., Kneese, T., Boyd, D.: Networked Employment Discrimination. Open Society Foundations' Future of Work Commissioned Research Papers (2014) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2543507
4. Solove, D.J.: A taxonomy of privacy. University of Pennsylvania law review, 477-564 (2006)
5. Kitchin, R.: The data revolution: Big data, open data, data infrastructures and their consequences. Sage, Los Angeles (2014)
6. Haynes, D., Robinson, L.: Defining user risk in social networking services. Aslib Journal of Information Management 67, 94-115 (2015)
7. Lyon, D.: Surveillance, power and everyday life. Emerging Digital Spaces in Contemporary Society, pp. 107-120. Springer (2010)
8. Clarke, R.: Introduction to dataveillance and information privacy, and definitions of terms. (1999) http://www.rogerclarke.com/DV/Intro.html
9. Lambiotte, R., Kosinski, M.: Tracking the digital footprints of personality. Proceedings of the IEEE 102, 1934-1939 (2014)
10. Pariser, E.: The filter bubble: How the new personalized web is changing what we read and how we think. Penguin, New York (2011)
11. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science 347, 509-514 (2015)
12. Christl, W., Kopp, K., Riechert, P.U.: How companies use personal information against people: Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information, Cracked Labs (2017)
13. Correia, J., Compeau, D.: Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA. Proceedings of the 50th Hawaii International Conference on System Sciences, Hawaii (2017)
14. Svantesson, D., Clarke, R.: A best practice model for e-consumer protection. Computer Law & Security Review 26, 31-37 (2010)
15. Torre, I., Sanchez, O.R., Koceva, F., Adorni, G.: Supporting users to take informed decisions on privacy settings of personal devices. Personal and Ubiquitous Computing 1-20 (2017)
16. Rotman, D.: Are You Looking At Me? Social Media and Privacy Literacy. 4th iSchool Conference, Chapel Hill, USA (2009) http://hdl.handle.net/2142/15339
17. Givens, C.L.: Information Privacy Fundamentals for Librarians and Information Professionals. Rowman & Littlefield, Lanham (2015)
18. Fereidooni, H., Frassetto, T., Miettinen, M., Sadeghi, A.-R., Conti, M.: Fitness Trackers: Fit for Health but Unfit for Security and Privacy. Connected Health Applications, Systems and Engineering Technologies (CHASE), 2017 IEEE/ACM pp. 19-24. IEEE, Philadelphia, PA, USA (2017) https://ieeexplore.ieee.org/document/8010569/
19. Clausing, E., Schiefer, M., Morgenstern, U.: Internet of Things: Security Evaluation of nine Fitness Trackers. AV TEST, The Independent IT-Security institue, Magdeburg, Germany (2015) https://www.av-test.org/fileadmin/pdf/avtest_2015-06_fitness_tracker_english.pdf
20. Ajunwa, I., Crawford, K., Ford, J.S.: Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs. The Journal of Law, Medicine & Ethics 44, 474-480 (2016)
21. Flybys: Small Steps, Big Impact. The path to a healthier lifestyle starts with just one step (2016) https://www.flybuys.com.au/collect#/partners/fitbit
22. Crawford, K., Schultz, J.: Big data and due process: Toward a framework to redress predictive privacy harms. Boston College Law Review 55, 39-92 (2014)
23. Floridi, L.: Four challenges for a theory of informational privacy. Ethics and Information technology 8, 109-119 (2006)
24. Barnes, S.B.: A privacy paradox: Social networking in the United States. First Monday 11, (2006)
25. Palen, L., Dourish, P.: Unpacking privacy for a networked world. SIGCHI conference on Human factors in computing systems 129-136 (2003) https://dl.acm.org/citation.cfm?id=642635
26. Nissenbaum, H.: Privacy in context. Stanford University Press (2009)
27. Nissenbaum, H.: Privacy as contextual integrity. Washington Law Review 79, 119 (2004)
28. Barocas, S., Nissenbaum, H.: Big data's end run around anonymity and consent. In: L. Julia, S. Victoria, B. Stefan, Helen, N. (eds.) Privacy, big data, and the public good: Frameworks for engagement, vol. 1, pp. 44-75. Cambridge University Press, New York (2014)

29. Sellen, A.J., Whittaker, S.: Beyond total capture: a constructive critique of lifelogging. Communications of the ACM 53, 70-77 (2010) https://dl.acm.org/citation.cfm?id=1735243
30. Hoy, M.B.: Personal activity trackers and the quantified self. Medical reference services quarterly 35, 94-100 (2016)
31. Barcena, M.B., Wueest, C., Lau, H.: How safe is your quantified self? Mountain View, CA: Symantec (2014)
32. Christovich, M.M.: Why Should We Care What Fitbit Shares-A Proposed Statutory Solution to Protect Sensative Personal Fitness Information. Hastings Communication & Entertainment Law Journal 38, 91 (2016)
33. Rawassizadeh, R.: Towards sharing life-log information with society. Behaviour & Information Technology 31, 1057-1067 (2012)
34. Wolf, G.: Know thyself: Tracking every facet of life, from sleep to mood to pain, Wired (2009) https://www.wired.com/2009/06/lbnp-knowthyself/
35. Lupton, D.: The quantified self. Polity Press, Malden, MA (2016)
36. Lupton, D.: Digital sociology. Routledge, London (2015)
37. Neff, G., Nafus, D.: The Self-Tracking. MIT Press, Cambridge, MA (2016)
38. Lupton, D.: You are your data: Self-tracking practices and concepts of data. In: Selke, S. (ed.) Lifelogging pp. 61-79. Springer VS, Wiesbaden (2014)
39. Lo, B.P., Ip, H., Yang, G.-Z.: Transforming health care: body sensor networks, wearables, and the Internet of Things. IEEE Pulse 7, 4-8 (2016) https://ieeexplore.ieee.org/document/7387856/
40. United States Federal Trade Commission: Internet of things: privacy and security in a connected world. (2015) https://www.hsdl.org/?view&did=805589
41. Foucault, M.: Discipline and punishment: the birth of the prison. Edited by Alan Scheridan, New York: Vintage (1977)
42. Doherty, Caprani, N., Conaire, C.Ó., Kalnikaite, V., Gurrin, C., Smeaton, A.F., O'Connor, N.E.: Passively recognising human activities through lifelogging. Computers in Human Behavior 27, 1948-1958 (2011)
43. Lewis, S.J.: Assessment of the Privacy and Security of Smart Toys Marketed to Children. Top10VPN (2017) https://www.top10vpn.com/wp-content/uploads/2018/02/Top10VPN-smart-toys-safety-report.pdf
44. Rahman, M., Carbunar, B., Banik, M.: Fit and vulnerable: Attacks and defenses for a health monitoring device. https://www.ieee-security.org/TC/SP2013/posters/Mahmudur_Rahman.pdf
45. Zhou, W., Piramuthu, S.: Security/privacy of wearable fitness tracking IoT devices. 9th Iberian Conference on Information Systems and Technologies (CISTI):IEEE. pp.1-5, pp. 1-5. IEEE (2014) https://ieeexplore.ieee.org/document/6877073/
46. Boam, E., Webb, J.: Qualified self going beyond quantification. Designmind. (2014) https://designmind.frogdesign.com/2014/05/qualified-self-going-beyond-quantification/
47. Michael, K.: Implantable Medical Device Tells All: Uberveillance Gets to the Heart of the Matter. IEEE Consumer Electronics Magazine 6, 107-115 (2017) ieeexplore.ieee.org/document/8048728/
48. Campos, H.: Fighting for the right to open his heart data:Hugo Campos at TEDxCambridge 2011. (2011) https://youtu.be/oro19-l5M8k
49. Hinckley, D.: This Big Brother/Big Data Business Goes Way Beyond Apple and the FBI. Huffpost (2016) https://www.huffingtonpost.com/david-hinckley/this-big-brotherbig-data_b_9292744.html
50. World Economic Forum: Rethinking Personal Data: Strengthening Trust. (2012) http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf
51. Pingo, Z., Narayan, B.: When Personal Data Becomes Open Data: An Exploration of Lifelogging, User Privacy, and Implications for Privacy Literacy. In: Morishima A., R.A., Liew C. (ed.) Digital Libraries: Knowledge, Information, and Data in an Open Access Society, vol. 10075, pp. 3-9. Springer LNCS (2016)
52. Bryman, A.: Social research methods. Oxford university press, Oxford (2015)
53. Bazeley, P.: Qualitative analysis with NVivo. Sage, London (2007)
54. Rainie, Lee, Duggan, M. "Privacy and Information Sharing" Pew Research Center, (2015) http://www.pewinternet.org/2016/01/14/2016/Privacy-and-Information-Sharing/
55. Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. Proceedings of the 5th ACM conference on Electronic commerce. ACM: pp. 21-29. (2004) https://dl.acm.org/citation.cfm?id=988777
56. Bandara, R., Fernando, M., Akter, S.: Is the Privacy Paradox a Matter of Psychological Distance? An Exploratory Study of the Privacy Paradox from a Construal Level Theory Perspective. Proceedings of the 51st Hawaii International Conference on System Sciences, Hawaii (2018) https://scholars.uow.edu.au/display/publication116721
57. Wernke, M., Skvortsov, P., Dürr, F., Rothermel, K.: A classification of location privacy attacks and approaches. Personal and ubiquitous computing 18, 163-175 (2014)
58. Case, D.O., Given, L.M.: Looking for information: A survey of research on information seeking, needs, and behavior. Academic Press, San Diego (2017)
59. Briedis, M., Webb, J., Fraser, M.: Improving the Communication of Privacy Information for Consumers. Australian Communications Consumer Action Network (2016)
60. Terms of Service Didnt Read: "I have read and agree to the Terms" is the biggest lie on the web. We aim to fix that. (2017) https://tosdr.org/blog/tosdr-in-action-i-have-read-and-agree.html

61. Tailor, N., He, Y., Wagner, I.: POSTER: Design Ideas for Privacy-aware User Interfaces for Mobile Devices. Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pp. 219-220. ACM, Darmstadt, Germany (2016) DOI: https://doi.org/10.1145/2939918.2942420