Parents unwittingly leak their children's data: a GDPR time bomb?

Suzanne Prior
Natalie J. Coull

Prior, S. & Coull, N.J. (2020) 'Parents unwittingly leak their children's data: a GDPR time bomb?' In A. Moallem (ed.), *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24 2020, Proceedings*. Springer, 2nd International Conference on HCI for Cybersecurity, Privacy and Trust, Copenhagen, Denmark, 19-24 July 2020.

The final authenticated version is available online at https://doi.org/10.1007/978-3-030-50309-3_31

Parents Unwittingly Leak Their Children's Data: A GDPR Time Bomb?

Abstract. There are many apps available for parents that are designed to help them monitor their pregnancy or child's development. These apps require parents to share information about themselves or their children in order to utilise many of the apps' features. However, parents remain concerned about their children's privacy, indicating a privacy paradox between concerns and actions. The research presented here conducted an analysis of parenting apps alongside a survey of parents to determine if their concerns regarding sharing information about their children was at odds with their use of parenting apps.

A survey of 75 parents found that they had strong concerns around the availability of information about their children but were using apps within which they shared this information. Parents were not giving consideration to the information requested when using apps. This should be of concern to developers given the growing awareness of users' rights in relation to managing their data.

We propose new guidelines for app developers to better protect children's privacy and to improve trust relationships between developers and users.

Keywords: Privacy, Security, Mobile Apps, Parenting

Introduction

Jack's mum shares information about her son's ADHD using a child development tracker and social network app. Eight years later she wants to enroll her child in an exclusive private school. Unbeknown to her, they search online to find evidence of behavioural issues before they decide whether or not to admit him. They find the original posting, and the ensuing discussion where others give her behavioural advice. The school decides not to admit her child.

Pregnancy and the experience of becoming a parent is a life changing event and in this digital age it is not surprising that parents look to online resources and mobile applications to provide them with information and support during this period (Prior, 2016). Mobile application developers have responded to this and there are apps for a large variety of parenting issues from conception to pregnancy development, contraction monitors and baby development trackers. Parents are becoming used to sharing information about their children before they are even born (Lupton and Pedersen, 2016).

However, by sharing information about their children through these apps, parents are unwittingly creating a digital footprint for their child and potentially compromising their child's privacy. Recent breaches in privacy in apps such as Sitter (an app used for hiring babysitters), in which information including address, credit card details and information on users' children were leaked in a data breach highlights the potential risks in having this information stored online, even in trustworthy apps. (Abel, 2018)

At the same time parents report being concerned about what information is available about their child online (Madden et al., 2012). This research seeks to build on previous work in the area of sharing children's information on social media, and in the security and privacy of mobile health

applications to examine how parents' views of privacy match with the mobile apps they install and use on their phones and the permissions they grant to these apps.

By better understanding how parents' concerns may impact on their use of these apps there is the potential for designers and developers of parenting apps to reach out to parents by including usable security and privacy measures which are clear and straight forward for users. These could be applied in similar manner to other HCI guidelines such as accessibility.

Related Work

Parenting and Privacy

In recent years there has been an increasing interest in parenting and data privacy within the HCI community (Ammari *et al.*, 2015; Moser, Chen and Schoenebeck, 2017).

Previous work in the field has looked at the information teenagers and children share about themselves on social media, and the implications this has on their privacy (Marwick and Boyd, 2014; Silva *et al.*, 2017). There has been a growing awareness in recent years, particularly as the digital native generation has aged and become parents of young children themselves that parents are increasingly sharing private information about their children with online audiences.

Much of this work has been conducted from a sociological perspective and examined sharenting – a term used to describe parents who over share information about their children online. There have been concerns over how children of so called "mummy bloggers" (professional bloggers who post regularly about parenting and updates on their children) may feel in the future when reading posts about themselves (Blum-Ross and Livingstone, 2017; Orton-Johnson, 2017). One large study looking at Facebook sharenting was conducted by Marasli et al., (2016) who examined the Facebook profiles of 94 parents and looked at the information shared through these profiles about their children. The study considered the social implications of this information being shared but also briefly touched on the potential for the children to become victims of identity theft. However, hiding this information from so called "big data" companies can be a considerable challenge, Vertesei (2014) looked at the steps necessary to prevent corporations from discovering a pregnancy and likened the necessary steps to being similar to those used by people wishing to commit criminal acts.

There has also been research into the data theft implications of this information being shared. Brosch (2016) examined the Facebook profiles of participants and noted the significant number of parents uploading photos of birth certificates or sharing their child's date of birth. The risks in sharing this sort of information was discussed by Minkus et al., (2015) who crawled a large number of adult profiles on Facebook for evidence of children in their public profiles and then combined this with public records to identify information on the children. Minkus highlights the value of this information to a data broker. It is possible that parents are not aware of the dangers in sharing information about children online, Steinberg (2017) offers suggestions for protecting children's privacy and suggests that this model could be viewed in a similar manner to the "back to sleep" and second hand smoking campaigns of the 1990s and early 2000s. Most of the work done into sharenting to date has focussed on social media, however the growing availability of parenting and pregnancy apps means that these are increasingly becoming another avenue for parents to share information about their children with others.

Mobile Apps and Privacy

The number of apps available to provide information and guidance on a range of topics beginning at ovulation tracking through to pregnancy, childbirth and parenting continues to grow at a rapid rate (Lupton, Pedersen and Thomas, 2016). According to market research from 2013, pregnancy apps are more popular than fitness apps (Dolan, 2013), and while there has been less research done into this recently it is thought that their popularity continues to grow (Haelle, 2018). It is possible that parents feel that by searching for information, sharing images and monitoring the development of their children they are performing good parenthood (Lupton, Pedersen and Thomas, 2016) and there is an increasing awareness that users are sharing a large volume of information through these mobile apps.

There has been interest in the amount of information being shared in mHealth apps (mobile phone apps related to health) in general for several years. One concern since health apps began to appear was the trustworthiness of the information, however this has now grown into concerns regarding the security of users' health information (Adhikari and Richards, 2014). It has been suggested that data breaches in mHealth apps are more common than might have been thought (Adhikari and Richards, 2014), and this may be due to a limited understanding of security and privacy in mHealth apps and the risks associated with this information being leaked (Dehling *et al.*, 2015). Plachkinova et al., (2015) created a taxonomy of mHealth apps in order to investigate their security and privacy concerns and suggest that information on privacy should be available in an app's description so that users can read it before downloading.

It is argued that the rush to produce mHealth apps has led to some aspects of privacy and security not being considered (Martínez-Pérez, de la Torre-Díez and López-Coronado, 2014). At the same time there appears to be a paradox in that users have high concerns about their privacy online but are also willing to trade their personal information freely when they feel there is a benefit to them (Wilson and Valacich, 2012). It is still not clear whether this paradox is due to users' desire for instant gratification and is a behavioural mechanism which cannot be altered (Acquisti and Gross, 2006), or a case of learned helplessness. Learned helplessness describes a situation in which users feel that it is inevitable that at some point their data will be compromised and as a result feel there is no point in taking privacy protecting actions (Shklovski *et al.*, 2014).

Research into privacy concerns surrounding parenting apps has been more limited than general mHealth apps, however it is now a growing concern. An Australian study found that many women using pregnancy apps were not concerned by the privacy of the information shared or the accuracy of the information they receive (Lupton and Pedersen, 2016). Lupton (2016) argues that monitoring apps related to conception and pregnancy may have been created for the purpose of acquiring data for data breaches. There is a risk that by sharing information in order to use apps, parents and their children could effectively become recruited as unpaid contributors to the "digital labour workforce" (Lupton and Williamson, 2017).

This study examines the links between the security concerns of parents when considering sharing information about their children, and the information they are willing to provide in order to use parenting apps. It differs from previous studies such as Lupton and Pedersen's work (2016) in that it is targeted specifically at users of parenting and pregnancy apps and looks at a wider range of privacy issues.

In this study we will investigate the extent to which parents are aware of the interaction between data sharing on apps and their privacy and propose the following hypothesis:

H1. Parents are conscious of security and privacy dangers in sharing information about their children.

H2. Parents with privacy and security concerns install, use and grant permissions to apps on their mobile phone without considering the security implications.

H3. Parents do not consider data sharing implications while selecting and installing apps.

Using these hypothesis, we look to answer the research question, what consideration do parents give to security and privacy concerns when installing parenting apps?

Methodology

In this present study, we explore the extent to which parents consider the security and privacy implications of providing data about themselves and their children in mobile apps and whether this influences the decisions they make about installing apps related to pregnancy and parenting.

A two stage approach was taken within this study. Firstly a poll was conducted with members of online parenting groups to discover popular parenting and pregnancy apps. This was combined with an analysis of trending Apps for Parents from the App Store.

The initial poll involved asking members of Parenting Facebook Groups which apps they used, and collating those responses. This was then followed by a survey of users of these apps to determine the extent to which they consider the security implications when installing apps.

App	App Description (Android Downloads)
Peanut	Peanut is a social networking app, designed to help mothers connect with, and learn from, other mothers in their local area. (50,000).
Ovia Parenting	Ovla Parenting is designed to help parents keep track of their child's milestones and provides advice on child development and parenting. Parents can use the app to share information about their children, including photographs and videos. (100,000).
Mush	Mush is a social networking app, designed to help mothers to meet similar, like minded-mothers in their local area. (100,000).
Baby Center	Babycenter produce a pregnancy tracker and baby development calendar app for parents. The app contains parenting advice and tips. (10, 000,000).
Sprout	Sprout is a pregnancy tracker with some premium content available for a fee, for example health information and 3d videos of in-utero foetus development. (1,000,000).
Bounty Parenting	Bounty Parenting is a pregnancy and baby tracking app, with vouchers and free samples available for pregnancy and baby related products, and links to UK relevant health guides and hospital information packs. (100,000).

Ovia Pregnancy	Ovia lets users track the development of a foetus and provides further advice and information on pregnancy and health tracking. (1,000,000).
Parentune	Parentune is a social networking app for parents, and provides access to parenting experts and online advice. (500,000).
Glow Baby	Glow Baby is designed to help parents track their baby's activities, including breast/bottle feeds, diaper changes, nap times and duration, medication, and record milestones. (100,000).
Glow Nurture	Glow Nuture is a pregnancy tracker, designed for expectant parents to track the growth of the foetus and provide advice on pregnancy related health matters. (500,000).
What to Expect	What to Expect is a pregnancy and baby tracking app to help parents keep track of foetal development and record their baby's milestones. (1,000,000).

Table 1. Apps Selected for Study

App Analysis

Eleven of the most popular parenting apps were selected for this study. These apps were then further analysed to ascertain which data types the apps requested during registration, and to review the terms and conditions of these apps. All of the apps were available through Google Play or the Apple Store.

The identified apps are shown in Table 1, along with a description of the purpose of the app.

We installed these apps onto our own personal mobile devices (one Android and one iOS), and logged the data that each app requested during the registration process. Table 2 shows the data that each app requested from the user.

Data Collected by Apps.

It is evident from Table 2, that there is a very broad range of data collected by the various apps. Some of the data requested relates exclusively to the user, for example name, email address and photo, while other data types relate to the user's child(ren), for example child's date of birth, child's medical history, and child's place of birth. To appreciate the sensitivity of the different data types, we further categorised the data depending on the longevity of the data. For each data type stored by the app, we categorised the data type depending on whether the data was static (i.e. would not change during the course of the owner's lifetime), flexible (may change over time) or dynamic (likely to change frequently). If there was a data breach, static and flexible data will be of more value in constructing a further attack on a victim, as the data is more likely to be accurate and useful in generating an attack hook that could appear authentic to the victim. In Table 2, the static data types have been coloured red, flexible as orange and dynamic as green. Some of the data could be considered publicly available, (e.g. if the data is already available in the public domain, e.g. from websites such as 192.com), while others would be considered private. For each of the data types, those considered private (i.e. not generally shared online or via social media) are denoted by (P).

Some of this information is considered private by certain organisations, and used to confirm identity (e.g. date of birth, place of birth).

Privacy Threats from Apps.

Privacy threats relating to the use of parenting apps include: a breach of user confidentiality, failure to protect the data, and client or server end bugs that could lead to a security breach. Given the sensitivity of some of the data collected, it is important that users are fully aware of what data is being collected, how and where it is being stored, and how the data is going to be used. We reviewed the Privacy Policies of each of the apps, to ascertain where data was stored and how it was used. Typically, the paid apps had the best level of privacy protection, where the user's data was generally stored only on the user's phone. This would ensure that a breach of the organisation's infrastructure would not lead to compromisation of the user's data, and the data was not being passed to third parties for marketing purposes.

Any threats to the user's privacy from these types of apps is limited to app security on the device itself, and the ease with which malicious apps installed on the device may be able to access the data on the device. The free apps stated various levels of data sharing within their privacy policies, with all of them requesting permission to store user data on the organisation's servers, with that data being passed to third parties for marketing purposes. Typically, the social media apps required the user to agree to share their data with other users.

Based on the information that is stored by these apps, a list of potential attacks that could be conducted using this information was compiled. A description of these potential attacks and how information could be used to help orchestrate such an attack is described below:

App	Peanut	Ovia Parenting	Mush	Baby Center	Sprout	Bounty Parenting	Ovia Pregnancy	Parentune	Glow Baby	Glow Nurture	What to Expect
Your name	X	X	X	X		X	X	X	X	X	
Your child's name	X	X	X	X	X	X	X	X	X		X
Current location (P)	X	X	X								
Address	X	X	X			X					
Email Address	X	X	X	X		X	X	X	X	X	X
Phone number (P)								X			

Your Photo	X	X	X	X		X	X	X	X	X	
Your child's photo	X	X	X	X		X			X		
Your date of birth		X	X			X		X			
Child's date of birth	X	X	X	X		X	X	X	X	X	X
Your child's due date (P)			X	X		X	X	X	X	X	X
Your contacts (P)								X			
Your social media profiles	X	X	X				X	X			
Your medical history (P)							X			X	X
Your child's medical history (P)		X					X		X	X	
Your child's place of birth (P)						X	X				

Table 2. – App Analysis

Spear phishing is an email spoofing attack that targets a specific user or organisation, using information that has been harvested to make the email look more authentic. Spear phishing emails are generally designed to gain unauthorised access to sensitive information, either by persuading the user to click on a link in the email or open a malicious attachment. If someone's email address was leaked from a parenting app, along with other personal information, this information could be used to construct an authentic looking spear phishing attack.

Identity fraud can occur if personal information has been stolen, for example following a breach of user confidentiality. Information such as name, address, date of birth can be used to gain access to existing accounts, or used to obtain goods or services by impersonating the user to open new accounts.

If a user's details are breached, this information could be used to construct a password guessing attack, or reset a user's password if 'security questions' can be guessed. If a user's password hash has been stolen, user's details could be used to generate a password dictionary, unique to that particular user that could be used to then orchestrate a hybrid password attack.

It would be relatively easy for someone who was seeking access to children, or vulnerable mothers, to use the apps to gain access to this demographic for grooming purposes.

App Reviews

The reviews of the apps in Table 1 which were posted in both the Google Play and Apple App stores were examined for any mention of privacy or security. Over 500 reviews were examined, eleven reviews were related to security or privacy, these were spread across seven apps.

Three reviews mentioned issues in deleting data, either users could not work out how to delete their data, or having thought they deleted it they discovered that it was still stored by the app provider.

Four reviews expressed concern over the amount of data which was being collected, these reviews related to two apps. While many reviews revealed users' frustration at being forced to create a Facebook account to log into some apps only one review related this back to a concern around their personal privacy. Of the remaining three reviews, one raised concern around the other users of the app and how they were vetted, one commented that it was not easy to change the privacy settings of photos stored on the app and the remaining review stated that they liked not having to give special privacy permissions to install the app.

Survey

Following analysis of the parenting apps selected for the study, we conducted a survey of parents who used parenting apps to determine what consideration they gave to security concerns when using the apps.

Participants and Design

An online survey was used to gather parents' views on security, privacy and app use. The use of an online survey enabled us to reach a wider geographical area than would have been possible through other methods. The survey questions were trialled with seven participants prior to validate the survey and ensure there were no barriers to survey completion. The survey was designed to be completed in under ten minutes.

Recruitment

Participants were recruited to the survey over the period of one month between April and May 2018. Recruitment took place through a variety of online mediums including Twitter, Facebook groups targeted at parents and parenting websites (such as NetMums and BabyCentre). We were aware that some parents who used parenting apps may not use social media and so leaflets about the study were put in playgroups, parenting cafes and children's recreation centres in the local area.

Following the informed consent process there were four sections to this survey.

Demographics

Participants were asked for their age, gender, level of education, if they had children, if they used parenting apps and their country of residence. If participants selected no to either having children or using parenting apps they were excluded from the study. As the survey was examining the amount of personal information which participants are willing to share we deliberately avoided asking for information by means of which participants could be identified. This meant that the demographic information elicited was limited but still ensured that any themes in participant groups could be identified.

Use of Apps

Before participants were asked about their privacy concerns they were asked to identify which of the apps in Table 2 they used. There were eleven apps available for them to select and the option of none of the above.

Privacy Concerns

The questions on privacy concerns were separated into two sections. The first section asked questions relating to general attitudes to security and privacy on a five point Likert scale ranging from Strongly Disagree to Strongly Agree.

The second section looked specifically at the information participants were willing to share in order to use an app. The following information asked for by the apps were listed and participants rated on a five point Likert scale their level of comfortableness with sharing this information, ranging from Very Uncomfortable to Very Comfortable.

Reaction to Apps

The final stage of the survey revealed a grid which presented the types of information stored by each of the apps. Once participants had examined this grid they were asked whether they were comfortable or uncomfortable with this information being collected. Depending on their answer they were then directed either to a question asking why they felt comfortable sharing this information or to a question asking them given they were uncomfortable with this what they were likely to do with these apps in the future.

Ethical consent was sought and obtained by the authors' institution prior to the commencement of the survey. The survey asked for no identifiable information and provided details at the end on websites which could provide participants with further information on keeping their data private if they wished.

Variable Name	% (n)
Age	
18-25	9.33 (7)
26-35	60 (45)
36-45	29.33 (22)
46-55	1.33 (1)
Country	
United Kingdom	89.33 (67)
USA	6.67 (5)
Australia	1.33 (1)
Singapore	1.33 (1)
Ukraine	1.33 (1)
Education	
Did not complete HS	2.66 (2)

Completed HS	12 (9)
Some higher education	30.67 (23)
Undergraduate Degree	50.67 (38)
Postgraduate Degree	32 (24)
PhD	1.67 (5)

Table 3. – Participant Demographics

Results

Descriptive Statistics

During the month that the survey was available 101 participants began the study, 26 were excluded because they were either not parents or did not use parenting apps. In total 75 participants completed the survey. Of those participants 97% (*n*=73) were female. Participants were composed predominantly of the millennial generation, the majority of participants were aged between 26 and 35 see Table 3.

The participants were mainly from the United Kingdom with the remainder coming from USA, Australia, Singapore and Ukraine. Participants had a variety of educational experiences ranging from not completing high school to having a PhD . The majority of participants had at least an undergraduate degree. All participants in the study had used at least one app with the average being 2.6 (sd = 1.6). The most popular app used was Baby Center (52%, *n*=39).

Levels of concern

When asked how concerned they were about the data being collected and shared about themselves and their children, the participants were above neutral in their level of concern for every category - see Table 4. Participants were more concerned about the data being gathered about their children than they were about themselves. The highest average level of concern related to information being collected about children for advertising purposes (*n*=4.04), followed closely by concerns around who could see information about their children (*n*=4). When considering information being shared about their children, only three participants (4%) were completely unconcerned with the volume of information stored about their children online, and with whom could see it. One participant (1.33%) was completely unconcerned about the information stored about their child for marketing purposes.

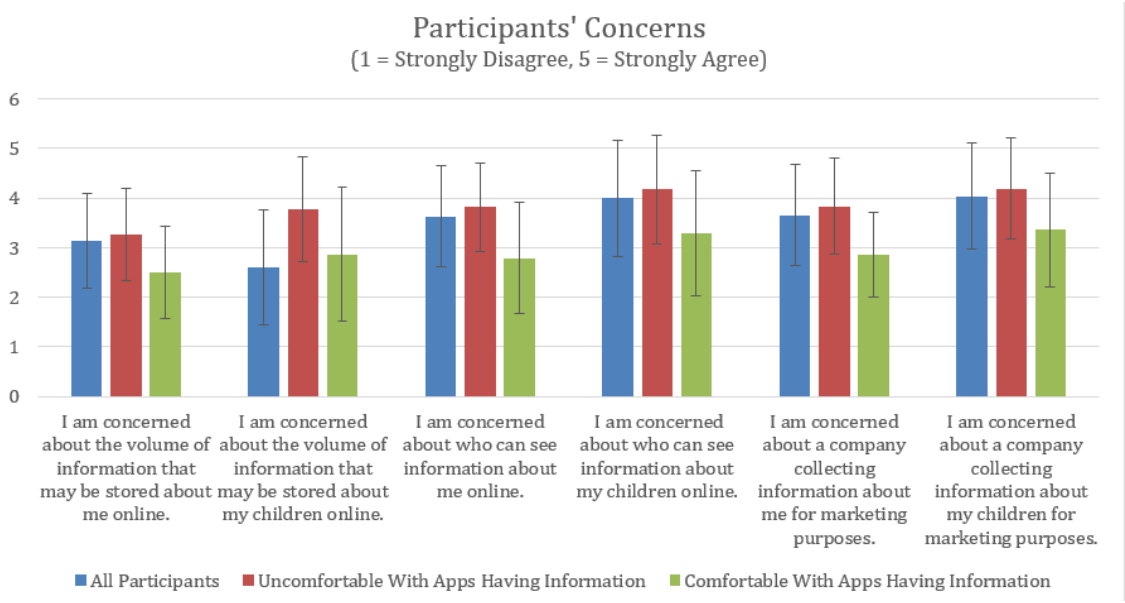

Fig. 1. - Participants Concerns Regarding Sharing Information

Levels of comfort

The examination of the information participants would be comfortable sharing revealed that there were only two categories of information in which participants on average rated feeling comfortable or very comfortable in sharing, these were their own name (*n*=3.45) and their email address (*n*=3.45). By contrast the average level of comfort for their child's name was 2.56. Participants were least comfortable in sharing their child's medical history (n=1.56), followed closely by their own medical history (n=1.6). The median for both these forms of data was 1.

Continued Use of Apps

Having been presented with the information regarding what information is stored by the apps, the participants were asked if they were happy to continue using the app, 81.3% of participants (*n*=61) were not happy.

Participants who were unhappy were asked about their future plans for use of these apps and the majority (65%, *n*=39) said that they would consider altering the settings on the apps. Only two participants (3.3%) planned to continue using the app as before and 31.7% (*n*=19) would consider deleting the app.

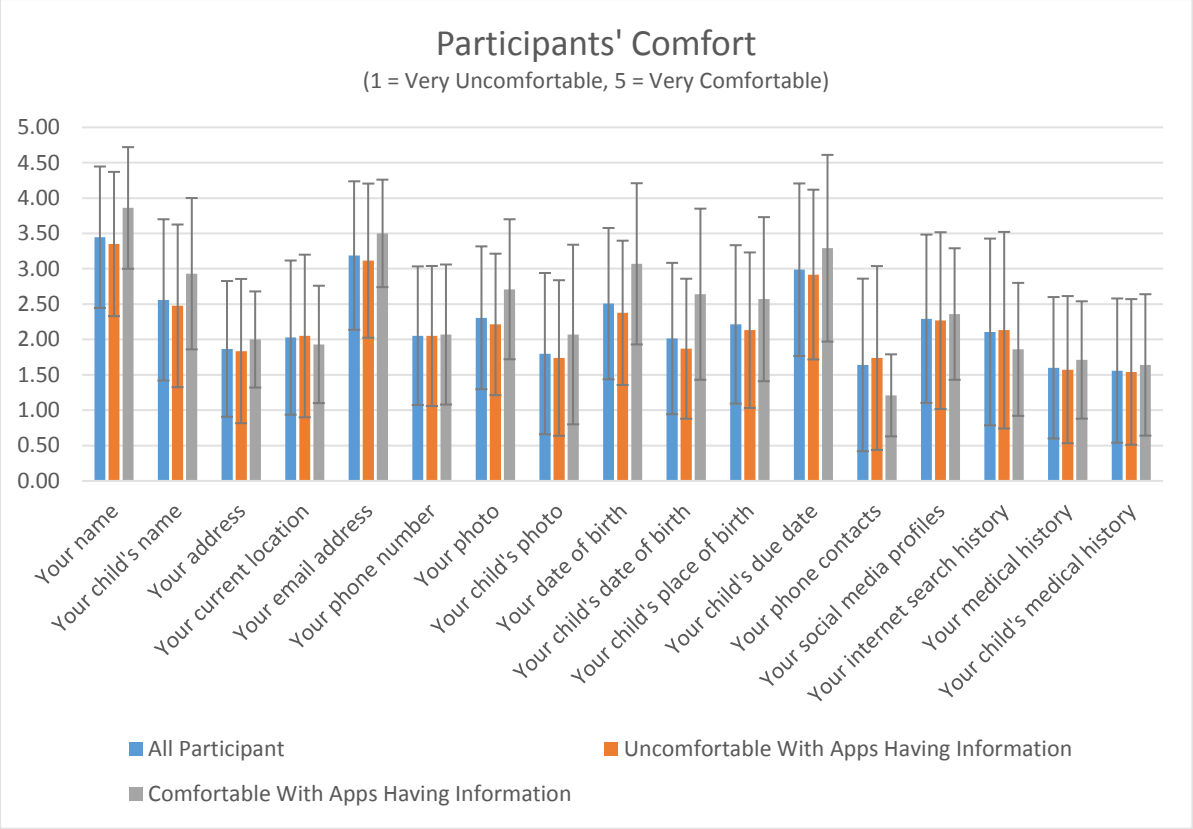

Fig. 2. – Participants Level of Comfort

The participants who were happy with the information being stored on the app were asked for the reason behind this. For the majority (78.6%, *n*=11) this was because they trusted the app providers to use the data appropriately, while the remaining three participants (21.4%) were not concerned about how this data was used.

By splitting the participants into two groups it is possible to examine any differences between them in their levels of concerns around issues about their data being shared and in their degrees of comfort in sharing specific forms of information.

In both cases the data was normally distributed and application of the MannWhitney U test shows that participants who were unhappy with the data being stored on the apps had reported higher levels of concerns around data sharing issues than the participants who were happy with the data stored on the apps ($z=3.01$, $p=0.003$). However there was no significant difference between their levels of comfort in sharing specific items of information ($p=0.14$).

Discussion

H1. Parent's consciousness of security and privacy dangers

Parents in the study on average were concerned about the information stored about them and their children. Areas of particular concern were who could have access to this information and how this information could be used for marketing purposes. This suggests they are conscious of the dangers in sharing information about their children.

H2. Installation and Use of Apps

There were no significant differences in the amount of information parents with high security concerns were potentially sharing through apps compared to those with lower security concerns. This indicates that despite having privacy and security concerns, parents are installing apps which request large amounts of information. It should be noted that this study did not specifically ask what information was being shared, but from our analysis of the apps we can conclude that this information would be required in order to use the app effectively.

H3. Sharing of Information

When participants were shown the amount of information that could be stored by the different apps they were using, 81.3% (*n*=61) they stated that they were uncomfortable with this and of these the majority (*n*=39, 65%) would be looking to change the settings on these apps. This indicates that parents are installing apps which request information about their children and are not taking on board that they are sharing information in doing this.

The results suggest that although the majority of parents are concerned by online security and privacy issues surrounding their children, they give little to no consideration to this when installing mobile parenting apps.

Hypothesis	**Supported/Not Supported**
H1. Parents are conscious of security and privacy dangers in sharing information about their children.	Supported
H2. Parents with privacy and security concerns install, use and grant permissions to apps on their mobile phone without considering the security implications.	Supported
H3. Parents are not conscious of the information they are sharing on apps.	Supported

Table 4. Hypothesis

Parents Views and Actions

Parents in the study reported being highly concerned about the information being shared about themselves and their children and uncomfortable with many types of information being shared. However, this appeared to be in contrast with their behaviour of using many apps which stored personal information on them. This privacy paradox has been noted in previous studies (Norberg, Horne and Horne, 2007), in which it has been noted that despite their disclosed intentions users frequently share personal data. Much of this previous work has looked at social media however, as this study has shown, this behaviour can also be found in the use of apps. This study's results are in contrast to those found in Lupton and Pedersen's work (2016) which found participants were not overly concerned with the data being stored or used by parenting apps.

One potential reason why this contrast can be seen so clearly in this study could have been due to stories in the media during the time period the survey was available. The Cambridge Analytica/Facebook scandal was first covered in the press in the UK in March 2018, shortly before

we deployed this survey and during the study was being discussed at on many popular parenting websites (babycentre, 2018; Mumsnet, 2018). The heightened awareness is often that users' data is a commodity may have explained this difference.

Guidelines for Developers

Those participants who responded that they were unhappy with the apps having their information indicated that they were likely to have been unaware of the amount of information being stored before the survey – only 3.3% would continue to use the apps with no changes. As pointed out by some commentators, by raising awareness of how data is processed there is the opportunity to build trust between app providers and their users. If user awareness in this area continues to rise then app providers may find themselves at risk of losing users if this trust is not present. Parental app providers could be at an additional risk, as this study shows parents are more guarded about their child's data than their own.

There are existing guidelines for developers regarding how much data they should request from and store about users. However, what our study suggests is that parents are particularly concerned about the amount of information being stored on their children and that should they become aware of this it may impact upon their use of the app.

We suggest that in addition to complying with current data legislation and only storing the minimum required amount of information, developers of parenting apps should work with parents to determine the levels of information they are comfortable in sharing with specific applications. Developers should also give consideration as to how they present the terms and conditions of their apps. If parents feel confident that they understand the digital footprint they are creating for their child then there is the possibility that they may be more inclined to continue to use the app.

In addition there may be benefits in allowing parents to use the apps without providing specific information about their child. For example will it affect the advice given by the app if they don't provide their child's gender or exact date of birth. Consider if there are less identifying ways to gather this data such as the child's age, could an icon be used instead of a photo of their child? Developers should give consideration to these issues when designing parenting apps.

Limitations

There are several limitations within this survey. Firstly by asking adults to self report on their concerns around data privacy there is the risk of a social desirability bias, we were not able to validate how accurate this reporting was. Secondly we did not investigate if parents who are concerned about the data being stored are actually sharing their child's data or using dummy data.

When asking participants about their comfort in sharing specific pieces of information this was on a very general form, there would be benefit in future studies examining in which situations they would be comfortable sharing these different pieces of information.

Finally we have not been able to follow up on the study to determine if the participants took any action after discovering the amount of data they were sharing.

Conclusion and Future work

There has been a large growth in recent years in pregnancy and parenting apps, and data on parents is of interest to many corporations. At the same time parents are becoming increasingly concerned

with what data is available online about their children and who can access this. This study has shown that despite these concerns many parents are using apps which store this information and have not given consideration as to who may have access to this information.

This survey showed that despite being unhappy with the information stored by app providers, the majority of participants were still planning to continue using the apps. However of those who were planning to continue using the apps, many would look to alter the settings on the apps, it should be noted that this is behavioural intention and it is not clear if it became actual behaviour.

Future studies should investigate if after being informed about the data stored by apps, participants make any changes to the settings on apps or the information, and if this has been influenced by the recent press stories regarding the commoditization of data. It would also be beneficial to work with parents who are non-users to discover any privacy concerns that have stopped them from using these apps.

References

Abel, R. (2018) *Babysitting app Sitter exposed the data of 93,000 customers*, *SC Media*. Available at: https://www.scmagazine.com/home/network-security/babysitting-app-sitter-exposed-the-data-of-93000-customers/ (Accessed: 19 November 2018).

Acquisti, A. and Gross, R. (2006) 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook.', in Danezis, G. and Golle, P. (eds) *Internation Workshop on Privacy Enhancing Technologies*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 36–58.

Adhikari, R. and Richards (2014) 'Security and privacy issues related to the use of mobile health apps', in *25th Australasian Conference on Information Systems (ACIS 2014)*. Auckland, New Zealand, pp. 1–11.

Ammari, T. *et al.* (2015) 'Managing Children's Online Identities: How Parents Decide What to Disclose About Their Children Online', in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM (CHI '15), pp. 1895–1904. doi: 10.1145/2702123.2702325.

babycentre (2018) *Cambridge Analytica and your social media use*. Available at: https://community.babycentre.co.uk/post/a31540953/cambridge-analytica-and-your-social-media-use (Accessed: 4 June 2018).

Blum-Ross, A. and Livingstone, S. (2017) '"Sharenting," parent blogging, and the boundaries of the digital self', *Popular Communication*. Routledge, 15(2), pp. 110–125. doi: 10.1080/15405702.2016.1223300.

Brosch, A. (2016) 'When the Child is Born into the Internet : Sharenting as a Growing Trend among Parents on Facebook', *The New Educational Review*, 43(1), pp. 225–235. doi: 10.15804/tner.2016.43.1.19.

Dehling, T. *et al.* (2015) 'Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android', *JMIR mHealth and uHealth*. Edited by G. Eysenbach. Toronto, Canada. doi: 10.2196/mhealth.3672.

Dolan, B. (2013) *Report finds pregnancy apps more popular than fitness apps*, *mobihealthnews*. Available at: http://www.mobihealthnews.com/20333/report-finds-pregnancy-apps-more-popular-than-fitness-apps (Accessed: 4 June 2018).

Haelle, T. (2018) *Pregnancy Apps: Your Patients Use Them—Are You Up to Speed?*, *Medscape*. Available at: https://www.medscape.com/viewarticle/892945 (Accessed: 4 June 2018).

Lupton, D. (2016) '"Mastering Your Fertility": The Digitised Reproductive Citizen', in McCosker, A., Vivienne, S., and Johns, A. (eds) *Negotiating Digital Citizenship:* United States: Rowman & Littlefield Publishers, pp. 81–93.

Lupton, D. and Pedersen, S. (2016) 'An Australian survey of women's use of pregnancy and parenting apps', *Women and Birth*. Elsevier, 29(4), pp. 368–375. doi: 10.1016/j.wombi.2016.01.008.

Lupton, D., Pedersen, S. and Thomas, G. M. (2016) 'Parenting and Digital Media: From the Early Web to Contemporary Digital Society', *Sociology Compass*, 10(8), pp. 730–743. doi: 10.1111/soc4.12398.

Lupton, D. and Williamson, B. (2017) 'The datafied child: The dataveillance of children and implications for their rights', *New Media & Society*. SAGE Publications, 19(5), pp. 780–794. doi: 10.1177/1461444816686328.

Madden, M. *et al.* (2012) *Parents, Teens, and Online Privacy*. Washington, USA. Available at: https://files.eric.ed.gov/fulltext/ED537515.pdf.

Marasli, M. *et al.* (2016) 'Parents' Shares on Social Networking Sites About their Children: Sharenting', *The Anthropologist*. Routledge, 24(2), pp. 399–406. doi: 10.1080/09720073.2016.11892031.

Martínez-Pérez, B., de la Torre-Díez, I. and López-Coronado, M. (2014) 'Privacy and Security in Mobile Health Apps: A Review and Recommendations', *Journal of Medical Systems*, 39(1), p. 181. doi: 10.1007/s10916-014-0181-3.

Marwick, A. E. and Boyd, D. (2014) 'Networked privacy: How teenagers negotiate context in social media', *New Media & Society*, 16(7), pp. 1051–1067. doi: 10.1177/1461444814543995.

Minkus, T., Liu, K. and Ross, K. W. (2015) 'Children Seen But Not Heard: When Parents Compromise Children's Online Privacy', in *Proceedings of the 24th International Conference on World Wide Web*. Florence, Italy: International World Wide Web Conferences Steering Committee (WWW '15), pp. 776–786. doi: 10.1145/2736277.2741124.

Moser, C., Chen, T. and Schoenebeck, S. Y. (2017) 'Parents? And Children?s Preferences About Parents Sharing About Children on Social Media', in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM (CHI '17), pp. 5221–5225. doi: 10.1145/3025453.3025587.

Mumsnet (2018) *MN, FB, marketing companies and our data*. Available at: https://www.mumsnet.com/Talk/site_stuff/a3199266-MN-FB-marketing-companies-and-our-data (Accessed: 4 June 2018).

Norberg, P., Horne, D. and Horne, D. (2007) 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors', *Journal of Consumer Affairs*, 41(1), pp. 100–126. doi: 10.1111/j.1745-6606.2006.00070.x.

Orton-Johnson, K. (2017) 'Mummy Blogs and Representations of Motherhood: "Bad Mummies"□ and Their Readers', *Social Media + Society*. SAGE Publications Ltd, 3(2), p. 2056305117707186. doi: 10.1177/2056305117707186.

Plachkinova, M., Andrés, S. and Chatterjee, S. (2015) 'A Taxonomy of mHealth Apps -- Security and Privacy Concerns', in *2015 48th Hawaii International Conference on System Sciences*, pp. 3187–3196. doi: 10.1109/HICSS.2015.385.

Prior, S. (2016) 'The Millennial Mum – Technology Use by New Mothers', in *Proceedings of British HCI 2016 - Fusion,*. Bournemouth, UK, p. 20.1-20.3.

Shklovski, I. *et al.* (2014) 'Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use', in *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM (CHI '14), pp. 2347–2356. doi: 10.1145/2556288.2557421.

Silva, C. S. *et al.* (2017) 'Privacy for Children and Teenagers on Social Networks from a Usability Perspective: A Case Study on Facebook', in *Proceedings of the 2017 ACM on Web Science Conference*. New York, NY, USA: ACM (WebSci '17), pp. 63–71. doi: 10.1145/3091478.3091479.

Steinberg, S. B. (2017) 'Sharenting: Children's Privacy in the Age of Social Media', *Emory Law Journal*, 66(4), pp. 839–884.

Vertesi, J. (2014) *My Experiment Opting Out of Big Data Made Me Look Like a Criminal*, *Time*. Available at: http://time.com/83200/privacy-internet-big-data-opt-out/ (Accessed: 11 June 2018).

Wilson, D. W. and Valacich, J. (2012) 'Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus', *International Conference on Information Systems, ICIS 2012*, 5, pp. 4152–4162.