ORIGINAL ARTICLE

DOI: 10.51480/1899-5101.16.1(33).5

What Does Google Opinion Rewards Require and Get from Users?

Ömür Talay
Akdeniz University, Antalya, Turkey
ORCID: 0000-0002-1633-6655

Hasan Cem Çelik
Akdeniz University, Antalya, Turkey
ORCID: 0000-0002-4157-7223

Abstract: This article focuses on the mobile app called "Google Opinion Rewards" (GOR), which is used as a data collection tool in market research and academic research. Developed by Google Surveys, GOR deals with voluntary participation of app users in data sharing in return for rewards. In this context, a test account was created in the GOR app to analyze the surveys, the app sent to the account for a period of three years. In-depth interviews were conducted with 12 participants from the USA, the UK and Turkey to gain comprehensive knowledge about the app ecosystem. The aim of the interviews was to understand the motivations of GOR users for using the app, and explore the counter-surveillance strategies users have developed to avoid surveillance. The findings indicate that most GOR users share their information recklessly even if they have security concerns and that users who are actively involved in surveillance, knowingly or unknowingly, and who want to maximise their income develop masking strategies against surveillance.

Keywords: communication; digital surveillance; counter-surveillance; data sharing; mobile apps.

INTRODUCTION

In March 2020, Matt Bryant, from Alphabet Inc.'s Google communications team, told Reuters they sent a Google Opinion Rewards (GOR) questionnaire to some users, asking them whether they had experienced flu-like symptoms in the past three days. Bryant explained the research was done at the request of Carnegie Mellon University (CMU) researchers who aimed to forecast the spread of coronavirus (COVID-19) infection. Bryant also emphasized that the data obtained from the participants would be aggregated and anonymized (Dave, 2020). Roni

Rosenfeld, co-leader of the CMU Delphi research group and head of the Machine Learning Department, stated that coronavirus cases could thus be forecast a few weeks ahead. Rosenfeld pointed out that they were extremely grateful for the support they received from Facebook, Google and their other partners, and that the data they provided were "invaluable". He also stated that, when they were capable of starting predictions for the deadly epidemic, their self-confidence would increase thanks to these data (Carnegie Mellon University, 2020).

Rosenfeld's describing the data as "invaluable" and "trust-building" for third parties makes questionable both the qualities attributed to these data and the nature of free mobile apps that mediate the use and transfer of personal data to third parties. Developed by Google Surveys (GS), a product of Google LLC, GOR, which is a 'market research' app through which users earn Google Play Credits by answering short survey questions or receive payments via PayPal. The application (henceforth—app) has been downloaded by more than 100 million users from mobile app markets, and it is just one of the free apps available in both Google Play and Apple's Store (Statista, 2021). Although the app is free for users, it could be they are paying with their data, because data collection is tightly associated with monetization (Cecere et al., 2020). Some previous studies on this topic (Book & Wallach, 2015; Demotriou et al., 2016; Meng et al., 2016; Razaghpanah et al., 2018) suggest free mobile app developers sell the personal data of their users to third parties. Many studies on free mobile apps that result in personal data leakage, and are therefore security problems themselves, have focused primarily on data leakage and security threats (Zhou et al., 2011; Gibler et al., 2012; Zhang et al., 2013; Ullah et al., 2014).

Another issue as that is just as important is that people *voluntarily* share with such apps their personal data, which they often avoid giving away, even to their closest relatives. In this context, this study aims to reveal GOR users' strategies for using the app and the main motives for voluntarily sharing their personal data with GOR in exchange for a reward, despite GOR carrying the risk of data leakage and invasion of privacy. In other words, the paper aimed to reveal the main motives for GOR users to behave like *app labourers* (iSlave, cf. Qui, 2014) serving Google products.

THEORY REVIEW

In today's information societies, monitoring, supervising and controlling the daily activities of people in order to measure the potential political, cultural and economic tendencies of people and manage market risks constitute a part of the capitalist entrepreneurial view. Sustaining the productivity and profitability of capitalist investments requires surveillance focused on personal data

(Lyon, 2001), and this results in mass collection and exploitation of personal data across various platforms. Zuboff (2019) asserts 'behavioral surplus' is obtained by surveillance capitalists seizing personal data.

In the twenty-first century, the increasing appetite for mass data collection generates a variety of opinions regarding the value attributed to these data. Data is the economy's new oil (Humby, 2006) or the currency of the internet economy (Gurria, 2008), which shows the significance of the value appraised to personal data. Zuboff (2019) disagrees in claiming that these nomenclatures are problematic as personal data are not mines but just exist in nature. Obviously, personal data exists in digital environments and communication technologies make it possible to keep it under surveillance and thus compete for it. Indeed, every new digital technological product is integrated into the existing surveillance technology. This dynamic activity introduces not only various types of, but also expands the scope of, surveillance (Lyon, 2001; 2007).

As individuals become dependent on communication technologies, digital surveillance reaches a critical highest level because individuals become subject to liquid surveillance (Bauman & Lyon 2013). Individuals can develop unique techniques to evade surveillance as they become more exposed to digital environments. Individuals, in their attempts to evade surveillance, are Marx (2003) claims, very inventive, which is manifest in various forms, particularly in digital realms. Indeed, individuals who devise evasive tactics invariably conduct counter-surveillance moves, which Burton (2007) argues are the processes of detecting and reducing scrutiny (Burton, 2007). Therefore, although digital environments serve as surveillance tools for governments and businesses, these tools also strengthen counter-surveillance capabilities (Kadivar, 2015).

Marx (2003) reveals that individuals have developed at least ten counter-surveillance strategies, of which the "blocking" and "masking" strategies. Individuals use these strategies to protect themselves from the possible negative consequences of activist movements such as political (Kornstein, 2019), citizen journalism (Ataman & Çoban, 2018) and video activism (Wilson, 2012), thereby reducing the negative effects of surveillance to the greatest extent possible.

On the other hand, when collecting large-scale personal data through mobile apps, users' awareness of the purpose for which their data is collected is minimal (Tay et al., 2021), and when installing a mobile app without detailed information or a partial acceptance option, users should only consent to third-party access (Karafiloski & Mishev, 2017). Even if mobile platforms such as Android warn users of the permissions requested by an app and trust that the user will make the right decision as to whether they should install the app, many users ignore the warning (Jorgensen et al., 2015). Users may also fail to understand the risks arising from the diversity of data kept in mobile devices, the use of multiple types of identifiers, the complex mobile app ecosystem, the limitations of app

developers, and the extended use of third-party software and services (Castelluccia et al., 2017). Thus, the assumption that users will understand the permissions requested before installing an app cannot go beyond wishful thinking (Jorgensen et al., 2015). At this point, Tay et al. (2021) argue inexperienced users who do not have sufficient information to comprehend and process the complexity of the permission and privacy information of an app, agree to install it intuitively without conducting a cost-benefit analysis (Tay et al., 2021). As users driven by their intuition become increasingly dependent for their daily activities and needs on mobile apps that record and store their personal data, not only do significant risks arise in terms of their security and privacy, but also they become the target of third parties (Arp et al., 2017; Polykalas & Prezerakos, 2019).

What is the role of users who are too lazy to evaluate the abovementioned risks from their own perspective and those who do not comprehend these risks adequately and, therefore, make intuitive decisions? Wenz et al. (2019) respond that "[t]hey have both active and passive roles". In this sense, users play an active role in this process while performing actions such as taking photos or responding to survey questions. The point to note here is that users have direct control over these actions. However, Bluetooth linkage to external device and GPS running in the background make the users passive and their control is minimized. Furthermore, although users may encounter privacy concerns (Jung et al., 2015; Ham, 2016; Segijn et al., 2021), most are not willing to fulfil the requirements of this concern[1]. This indifference, which is called the privacy paradox (Barnes, 2006; Kokolakis, 2017) has proven to be extremely common among mobile phone users (Zhou, et al., 2011; Shklovski et al., 2014; Taddicken, 2014; Gerber et al., 2018; Han et al., 2019; Sanchez et al., 2019; Afolabi et al., 2020). Indeed, even if they have serious privacy concerns, users become involved in surveillance by submitting their data to continue using the app and thus they destroy their privacy rights themselves (Bauman & Lyon, 2013). Most of the users who believe that this is the price for getting a "free" app will not see any issue in paying unless there is a negative outcome (Shklovski, et al., 2014; Book & Wallach, 2015; Meng, et al., 2016).

The prerequisite that makes users consent to such an arrangement is that it is not a paid-for app. In this sense, free apps have three possible solo or combined monetization in-app strategies: (i) advertising; (ii) purchases; and (iii) users' personal data. While in-app ads are mostly used by apps downloaded fewer than 100 million times, those downloaded more than 100 million times mostly

1 These requirements largely consist of paying attention to the access permissions of the app and reading the privacy policies and terms of service. However, the freedom to grant or deny access permissions is frequently not in the hands of the user because it is impossible to use many functions of the app without these permissions. Furthermore, the lengthy privacy policies and terms of service make them difficult to read and are often overlooked by users.

earn their revenues by selling personal data (Cecere et al., 2020). Various studies reveal that GOR and similar free mobile apps demand more access to personal data than paid apps (Hyrynsalmi et al., 2012; Leontiadis et al., 2012; Polykalas & Prezerakos, 2019), which strongly suggests that the business model of free mobile apps is based on personal data abuse: "When the mobile app is free, the product is your personal data" (Meng, et al., 2016; Polykalas & Prezerakos, 2019).

This is the case for GOR, which is an online survey app. Users answer questions on the mobile platform in return for credits for books, music, and apps, and they answer demographic questions when they initially download the app (Kanyadan & Ganti, 2019; Hogan et al., 2020). At this point, in the only study directly dealing with GOR, Fernandes and Oliviera (2020) found that the app collects users' personal data and earns money by sharing this data with advertisers, and this data can include information such as the user's device, location, search history and app usage. Users provide this data to Google by responding to surveys and are paid in return. However, this payment may be below the actual value of the user's data. In this study, we look at the GOR app from the users' points-of-view. Therefore, the questions this study seeks to answer are as follows:

- RQ1: What are users' GOR usage strategies?
- RQ2: What are users' biases and attitudes regarding GOR?
- RQ3: What are the primary motivations of GOR users to voluntarily share their personal data with GOR in exchange for a reward?

METHODOLOGY

This study, which aims to reveal GOR users' strategies for using the app and their main motivations for voluntarily sharing their personal data with GOR in exchange for a reward, utilized a phenomenology design, which is a qualitative research method. The design that focuses on phenomena that we are aware of but do not have an in-depth and detailed understanding of (Groenewald, 2004), is suitable for qualitative research because it aims to understand individuals' lived experiences and how they experience a particular phenomenon. Therefore, this design is particularly useful when it comes to gaining insights into subjective experiences (Donalek, 2004). There were three reasons for choosing the phenomenological approach as a qualitative research design and the in-depth interview method as a data collection method. First, it supports document analysis, and secondly it can reveal the details or problems that lie in the depths of the cases compared to quantitative studies, and thirdly it allows us to look at these cases from a multi-faceted perspective.

We started to form the data set of the article by creating an individual test account for GOR and storing the survey questions sent to us by the app as of 2017.

For three years 2017–2020, we answered the survey questions, took screenshots of them, and obtained a total of 150 surveys. We mapped the surveys, analysing the questions and their options. Afterwards, we conducted document analysis by combining the surveys sent to us and the screenshots of surveys shared by GOR users on Reddit, categorizing the intended use of these surveys. Finally, by diversifying the data collection method, we conducted in-depth interviews with 15 GOR users between the ages of 18 and 37 years, who used the GOR mobile app and reside in three countries (USA, UK, and Turkey). The prerequisite for us to select the participants for the in-depth interview was that they actively used GOR and shared the screenshots of surveys in Reddit.

In this context, criterion sampling was used to identify participants, which is extremely useful when specific cases are purposively sampled based on predetermined criteria (Sandelowski, 2000, p. 248). Via direct messages in Reddit, we asked users whether they would volunteer for an interview and out of 126 messages, there were 17 responses. We excluded users under the age of 18 years. Discovering that the comments made during the interviews were repeated—a clear sign of data saturation—we limited the number of the participants to 12 (4 participants from each of the three countries). Before starting the interviews, participants were informed about the subject and purpose of the study and were informed that their personal data would be kept confidential and that they could terminate the interview at any time.

Interviews with users were conducted on Discord which is instant messaging app. Each interview lasted approximately 30 minutes. All conversations that occurred during the interviews including those that were outside the scope of the study were first written in the interview form. These written data were then transferred to the NVivo 11 program, which facilitates the creation of categories related to the research topic for the researcher. Three main themes were identified, consisting of (i) the users' strategies to use GOR, (ii) their motivation to share their personal data on the app, and (iii) privacy concerns about their usage data. Analyses were carried out on these three main themes.

FINDINGS

After the GOR app was installed on the smartphone, we were welcomed by the survey trainer and the first survey started. The app warned us that the first survey was a paradigm of the types of surveys that would be sent and that there was no reward. Moreover, the app asked us to give true answers to the questions as the answers would determine whether we would be approved for receiving more surveys. The app then asked us to turn on the location history of the smartphone. Location history records the places smartphone owners travel

to with their devices even when they are not using any Google services. If location history is switched on, surveys about the places visited are sent. The app, thus had the prerequisite data for displaying personalized ads to users (Shoaibi & Rassan, 2012; Bauer & Strauss, 2016) because location share gives marketers an advantage in offering personalized ads to their customers. Afterwards, we were asked to approve the GOR Terms of Service (the screenshot of this section could not be stored due to the security policy), and the app informed us that we accepted the Google Payments Terms of Service by using the app.

USERS' STRATEGIES

When we evaluated the first survey of GOR, we found that the app measures the user's attention, and that answers to the questions establish the basis for surveys that will be sent later: The survey trainer measures the level of attention by first asking a control question and then proceeds to demographic questions involving languages spoken, age range and gender, the survey closes with a question of interest. Based on these data, GOR gradually gets to know the user and follows the paths opened by the data to show them more relevant surveys.

Every time the app sends a survey question to a user, it specifies the purposes for which the survey can be used and asks for the approval of the user. These purposes are as follows: (a) showing users more relevant surveys (providing new surveys based on demographics and interests); (b) showing more relevant ads (displaying personalized ads based on data obtained); (c) sharing data with the research organisation paying for the e-survey (ROPES), which targeted both GOR and GS plus selling collected data to the ROPES); and (iv) developing Google products by asking questions about Google products or the Google company.

Table 1 shows the categories we created by the thematic analysis of the data we obtained from in-depth interviews with the GOR users who shared on Reddit:

Table 1. Categorical coding of qualitative data in the interviews (N=56) ranked by frequency.

Category	Code	N
Location	My location history is on	13
Demographic	Gender and age	9
Area of interest	Sports I do	7
Purchasing behaviour	To display advertising	7
Psychological	Stress, anxiety	5
Google identification	Google Chrome, Google Maps	4
Political	Political trend	3
Health	Covid-19	3
Control question	You must answer correctly	3
Cultural	Reliance	2

The category frequency of the surveys sent to us and the ratio of these categories to the survey questions are shown in Table 2:

Table 2. Frequency and percentage distribution of categories in all the surveys (N=150) ranked by proportion (%).

Category	N	Proportion (%)
Location	61	40,67
Demographic	45	30,00
Area of interest	31	20,67
Purchasing behaviour	7	4,66
Google identification	3	2,00
Psychological	3	2,00
Control question*	1*	-

* not included in the calculation of N

Regarding the working principle of the app, we thought that GOR, after receiving the answers given to the demographic questions, was unlikely to ask such questions again. We were wrong, as the app continued to ask them. This was true not only for demographic questions, but also for the other categories such as "interests":

Table 3. Frequency and Percentage Distributions of Primary Survey Questions (N=150).

Primary survey questions	Category	Frequency (N)	Incidence of appearance in all 150 surveys (%)
Which of the following places have you visited recently?	Location	61	40,67
Which of the following sports do you watch?	Area of interest	24	16,00
Do you work in one of the following sectors?	Demographic	11	7,33
Which of the following categories best describes your job situation?	Demographic	10	6,67
Which of the following sports do you do?	Area of interest	7	4,67
Which of the methods of electricity generation for residential use do you know?	Purchasing behaviour	7	4,66
Are you a parent of a child who lives in the same house?	Demographic	7	4,67
What's your marital status?	Demographic	6	4,00
Is your house rented or owned by you?	Demographic	6	4,00
Are you currently a university student?	Demographic	5	3,33
Which of the following Google products have you used in the last 30 days?	Google identification	3	2,00
How many hours did you sleep each night on average last week?	Psychological	3	2,00
Which of the following are continents? *	Control question	1*	

* not included in the calculation of N

We can assume that GOR did so because the ROPES had set a long time frame for the duration of the survey, which could mean that the survey sent to the user can be repeated. In addition, we believe that GOR may be repeating the questions to enable its users to sustain their continuity and motivation because the alternative is dire for the app. An absence of surveys means there no user responses for the ROPES to audit and thus no new surveys to be sent to the user.

As for questions about location, we noticed that the app identified almost all the places we visited. The day after any store visit, we were subjected to questions regarding the precise location, such as: "Which store/brand did you visit?"; "When did you visit it?"; and "How did you pay?". At this point, we assume that credit card payment behaviour might be shared with credit card companies or ROPES paying for the user's current location:

> *The day after I visit a store, they send a survey. Mostly, they send the questions of "Which store have you been to at most?", "When did you go there?", and "How did you make your payment?". You meet someone… It's kind of starting to learn things about you. "What are your likes?", "What sports do you do?", or "Do you do your shopping in cash?" Do you use a credit card? By learning them, it's capturing your data – and in a way, capturing you. (P12. TUR).*

Given that GOR is a market research app, it is normal that it asks users questions to get to know them. However, receiving money or rewards in this trade also appears to reveal an employee-employer relationship. In some of Google's products (e.g., YouTube), consumers are referred to as "partners," but there is no similar declaration in GOR. Users create an implicit employee-employer relationship without any employment contract with GOR and generate added value in favour of Google, which shows us that users are exposed to exploitation of "immaterial labour"[2].

Parallel to exploring the demands that GOR makes from users and how it wants to get to know/identify them, we categorized and mapped the surveys sent to us as primary questions and their subcategories (See Figure 2). We noticed that, while many of the 150 survey questions were asked in the same way, some questions were asked in a way close to each other; even in some of them only the placing of some words were different. The findings from the in-depth interviews revealed that three participants expressed discomfort with being asked the same questions repeatedly:

> *It's like being called a liar and it bothers me. (P1. USA).*
> *Asking the same question persistently bothers me after a while. Even if I'm lying it's uncomfortable for him to hit me in the face. (P6. UK).*
> *I think GOR is testing whether I am honest or not. It measures whether I've given true answers to the questions, and whether my answers to the same questions asked at different times are consistent. It can't be so difficult for them to keep this data. (P10. TUR).*

Asking the same questions over and over to evaluate the users' behavior and discover the sort of attitude they might build in response is another aspect of behavioral surplus. The study of personal behaviour enables the forecasting of users' conduct, thus providing unique preliminary information for a prospective. A key finding from the interviews was that the more detailed the questions are in the surveys, the greater are the rewards, so that as one user states rather than giving the true answer, they may give deceitful answers in order to get follow-up questions:

---

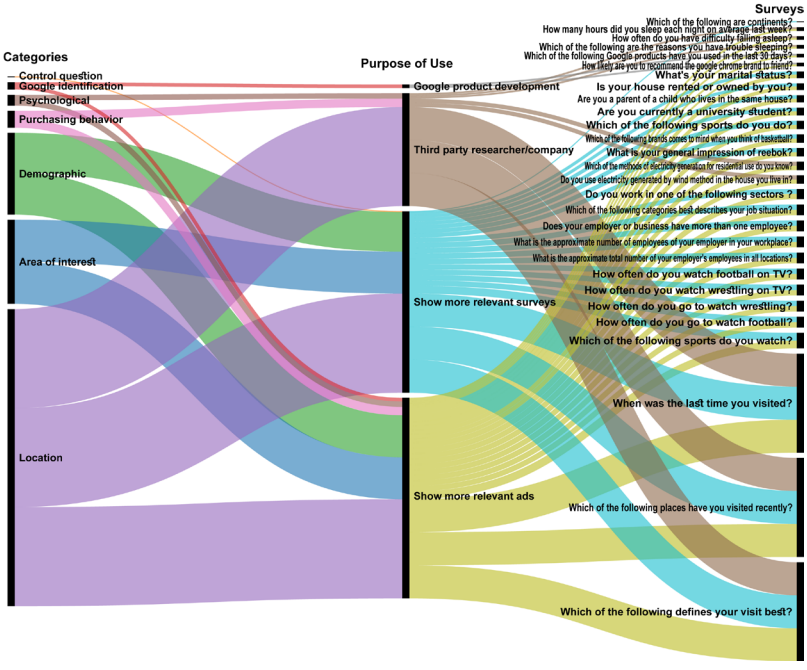
2 Immaterial labour encompasses tasks that are not generally considered employment (Lazzarato, 1996). New types of work have evolved in today's information society, and the workers who do these forms of labour, namely the labour of users, are exploited. People who spend time on digital platforms typically provide added value through their actions to organizations having these platforms. Given GOR users' relationship with the app, it would not be incorrect to suggest a substantially greater amount of labour exploitation.

> *The longer and more detailed the survey, the greater the reward. You cannot earn much money from the surveys that you've completed quickly. For example, if you answer "no" when asked "Do you play football?", the survey ends there, and you earn a tiny amount of reward. Say, if I earned a similar amount of reward each time I fill out a survey, I would tell the truth; I wouldn't extend the survey. More precisely, I wouldn't bother to extend it. If my reason for filling out a questionnaire is to earn a reward, it's normal for me to take advantage of every opportunity. (P9. TUR).*

Associations between Survey Questions, Categories, and Purposes of Use

We continued our analysis by examining the linear associations between GOR's purposes of use of survey questions, the categories we obtained from in-depth interviews, and the survey questions sent to us. We determined that some survey questions have more than one purpose of use, and that they were included in more than one category. Figure 1 shows all the questions (in categories and subcategories) sent to us:

Figure 1. Associations of Survey Questions Sent to us in terms of Categories and Purposes of Use.



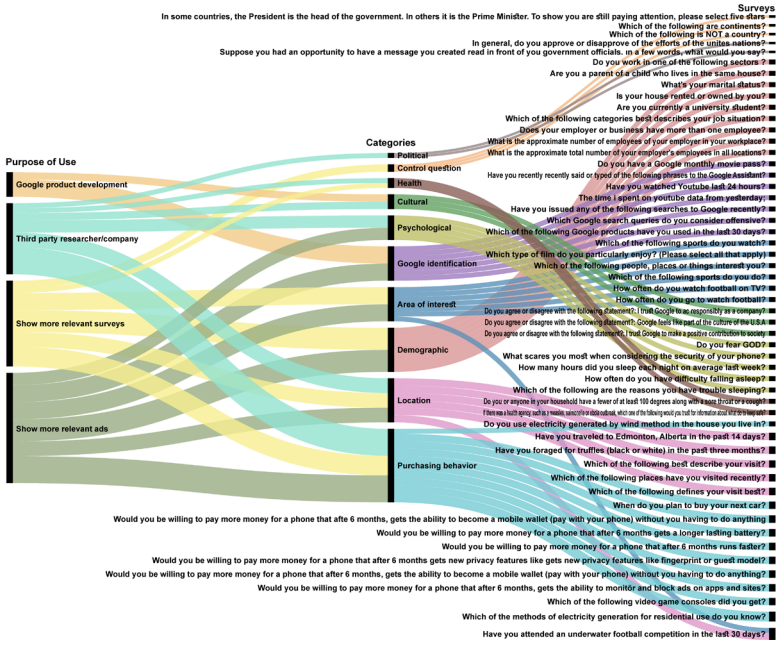
As shown in Figure 1, the category of "location" was associated with three purposes of use, while the questions regarding "interests" and "demography"

were associated with two purposes of use: It is evident that "location", "interests", and "demography" are the most convenient data collection categories for GOR. Among the demographic questions, the ones regarding age, gender, and marital status range are used to send more frequent and relevant surveys. The statement provided by one of the interviewees also corroborates this finding:

> *A few days after questioning my marital status, it learnt if I have a child, too. Since I don't have a child, certainly, it'll no longer show me any ads for diapers or ask a question about it. (P7. UK).*

Via Reddit and in-depth interviews, we found out that the questions in GOR surveys are not limited to those sent to us; on the contrary, they are asked in many ways and the variety of survey questions is constantly increasing:

Figure 2. Associations of Surveys Collected by Reddit and In-depth Interviews as well as Surveys Sent to Us in terms of Categories and Purposes of Use.



As shown in Figure 2, there are also categories (culture, health and political) not included in Figure 1. While the category of "purchasing behaviour" is associated with two purposes of use in Figure 1, it is associated with three purposes of use in Figure 2. In addition, with the increase in the questions associated with the category of "purchasing behaviour", its association with the purpose of use also diversified. There was also a rise in the questions regarding "location" and these questions were asked more specifically (Have you travelled to Edmonton,

Alberta in the last 14 days?). Similar to the questions regarding "purchasing" and "location", both the questions about "interests" and the variety of questions saw an increase. One of the differences at this point is that the question about "location" is associated with the relevant field (Have you attended an underwater football competition in the last 30 days?). Another remarkable question is "Are you afraid of God?", which we placed in the category of "psychological". Participants were asked to share their views about this question. Three participants stated that they had not encountered it, and yet if such a question were asked, they would not find it odd:

> *I think human psychology plays a role on whether someone will do shopping. If a person is afraid of God, he is generally a believer. If companies know you're a believer, this will strengthen their hand. (P3. USA).*
> *Whether you believe in God or not can affect some dynamics in human life, which must be the main reason why this question is asked. (P8. UK).*
> *OK, this question hasn't been asked OF me, but I wouldn't say "How dare they ask such a private question?". Nobody gives anything to anyone for free. If you don't want to answer it, you can just skip the question or ignore it. (P11. TUR).*

In essence, GOR's sole trump card is the reward that allows its users to reveal even the most private or deepest secrets; in addition to the data it gets through its hundreds of apps, Google acquires far more distilled information – even if this data is manipulated, they are significant for Google – in return for very small rewards.

MOTIVATIONS OF USERS TO SHARE THEIR PERSONAL DATA ON GOR

Bauman and Lyon (2013) note that we destroy our privacy rights voluntarily, or perhaps just consent to the loss of privacy as a price to be paid in exchange for the appealing elements offered to us. For them, only a few resilient people who do not act with herd mentality can make a sincere attempt against the app logic. As revealed in the in-depth interviews, it was clear that two participants were indifferent to sharing their personal data to win varying amounts of prizes.

> *I've handed over all my information for $20 in 5 months. Am I regretful? Of course not! (P5. UK).*
> *I made 50 TL (about $4) in a year. Considering that it took me 12 or 13 seconds to fill out a survey, it sounds like a good deal to me. (P11. TUR).*
> *Now that my data is useless, I think it's a nice trade-off to get paid apps for free. If I come across an app that pays money directly, I can give all my information and fill out a survey. (P12. TUR).*

PRIVACY CONCERNS OF GOR USERS

Based on our in-depth interviews and our findings on the importance of demographic questions, we asked the participants "Do the questions about your demographic data asked by GOR raise any privacy concerns for you?". The participants' views, as captured in the in-depth interviews, corroborate the notion that although they have privacy concerns, one Turkish and one UK participant have not developed a defense against the current privacy violation:

> *Privacy? According to whom? To me, there is no such thing as privacy. They even know where I live… If Google were my next-door neighbour, I guess it wouldn't have that much information. (P8. UK).*
> *This makes me worried about privacy, that's for sure. But since you first started using a smartphone, they've been storing almost all your data. Let's say, I didn't use this app; I use Gmail, I use Chrome, I use Google Maps. Even if I get concerned, I realize it is an unwarranted worry. (P9. TUR).*

As the preceding statements demonstrate, people who use Google and its products have the misconception that, if they use any Google product, their information has already been collected, and that it is useless to take measures to prevent any app they use from accessing it.

According to the findings from the in-depth interviews, two participants who think Google cannot be cheated believe that this will be noticed in the future, and after a while, the app will stop sending surveys. This attitude of the participants provides a summary of the idea that Google surveillance cannot be resisted. It is also evident that the barrier to resistance to surveillance is the outcome of accustoming people to personal data extortion and invasion through a kind of combination of helplessness and surrender, as Zuboff (2019) put it in the "Cycle of Dispossession"[3]:

> *You can't cheat Google. Like it doesn't know who you are. At least, it knows your age range. (P4. USA).*
> *I don't think Google can be tricked. First of all, the operating system used belongs to Google. It has an app market and also hundreds of apps. I search in Chrome… I use Google Maps… Many apps that are integrated with each other. (…) you'll get caught out finally. (P5. UK).*

3 Dispossession, according to Zuboff, imposes a new kind of control over people, masses, and society. As the corporation learnt how to counter and transform public resistance as a necessary prerequisite for the protection and expansion of its behavioural surplus franchise, the theory and practice of dispossession were developed and perfected.

On the other hand, masking themselves is the only anti-surveillance strategy for the users who voluntarily download the GOR app and are actively involved in surveillance—wittingly or unwittingly. Blocking and masking moves are common especially in communicative surveillance. By blocking, subjects seek to make communication physically inaccessible or useless (Marx, 2003); however, masking is more widely used in volunteer surveillance. Another reason why users are not concerned with the surveillance in this system, in which they voluntarily engage, may be because they believe they are masking and hiding themselves.

In this context, one interviewee thinks that GOR can be manipulated in order to win more prizes. Immediately after installing the app, users set up their demographic information in such a way they can receive more survey questions, which shows that users develop a strategy unwittingly to evade surveillance by masking themselves:

> *This app can be tricked sometimes. Some of my friends are trying to be someone the app wants; more precisely, they give deceitful information and try to get more follow-up surveys. For example, while installing the app, he signs up as a young female… He acts as if he had a high income, someone constantly shopping… Because he believes he will get more surveys if he acts like that. (P9. TUR).*

DISCUSSION

In this section, we discuss the analytical perspectives of our approach and evaluate the results. Our first aim was to analyse GOR's initial survey. Our analysis showed that the first survey set the ground for subsequent survey questions. However, based on the data obtained from the participants, the striking aspect was that the app contains a system which is vulnerable to manipulation in terms of demographic data. There is a variety of information in Reddit showing how the GOR app can be tricked. Basically, participants agree that when they provide misleading demographic information, they can get more survey questions and, as a result, they can earn more rewards. Furthermore, users who wish to maximize their revenues in GOR unwittingly utilize a counter-surveillance tactic, masking themselves to prevent surveillance.

Google provides ROPES that use the GS product with the option of collecting data by targeting GOR while creating a survey (Google Surveys Help, 2021). The demographics of the users targeted by using GOR can be determined in line with the sample of the researchers; demographic metrics such as country-region (the countries that can be targeted with GOR as of 2020 are Australia, Brazil, Canada, Germany, Italy, Japan, Mexico, Holland, UK, and the USA), language,

age, and gender can be used to narrow down the targeting. In addition, on the website of Google Surveys Help (2020), GOR's target audience is defined as users who tend to use technology more and are more likely to be young and male. There expected sampling biases such as, in comparison to the general population, GOR users are described as highly educated, physically active, less likely to own a home and visit a doctor, and more likely to own or use a DVR or video-on-demand. However, it is controversial to what extent this demographic information is provided truly or completely by the users.

This is a possibility even for our interviewees. Therefore, in addition to demographic information, it is unclear to what extent the answers given to the survey questions reflect reality. Moreover, information on the GS website indicating that GOR users are well-educated in comparison to the general public contradicts concerns about privacy and the low amounts of rewards. From another perspective, as previously indicated, users deceive the program by presenting themselves as highly educated suggests that the expected user profiles of GS are unfounded.

When we analysed GOR's survey questions and answers, we found some findings about the repetition of several questions. Although asking the same questions at different times is a strategy to detect changes in the general opinion of the public over time (Pew Research Center, 2021), we believe that this may be due to GOR's intention to confirm previous answers given to survey questions. Alternatively, it could be an experimental development process for machine learning or artificial intelligence. In addition, we found some findings that the repetition of questions puts pressure on users loyal to the app, which can create a feeling of a control mechanism on the users that is mostly unnoticeable.

On the other hand, the aspect that the questions in GOR are brief and relatively easy to answer indicates that they are in accord with GOR's short survey policy, and that they can motivate the user with shorter and more frequent surveys. One can assert that placing "I don't want to answer" and similar responses among the options of almost all the survey questions is nothing more than an effort to give the impression that GOR cares about the privacy of its users. Especially, as we know that GOR is aware that the user knows the survey will end if they chose this response. In addition, one must bear in mind that users' refraining from answering questions creates data for Google as well. The existence of branding strategies included in the answers to the survey questions is not surprising at all, considering that GOR is basically built on the strategy of getting to know and identifying the user.

Our second aim was to examine the association between survey categories and purposes of use. We noticed that the questions in the category of location were frequently asked. The aspect we found intriguing is that, although Google mostly knows the user's location precisely, it still asked "Which store did you visit?" and "When did you visit there?". The reason why GOR is asking these

questions is a means to ask the real question. The data GOR is interested in is the answer to the question "How did you make the payment?", which is under the category of "location". This is because GOR mostly does not need passive data collection methods to learn offline purchasing behaviour and decision-making mechanisms of the user. In addition, it is evident that demographic data, which includes age-gender, marital status, income status, parental status, and the user's residence information, is one of the most influential data categories delivered to GOR in terms of determining which ads will be displayed to the user. Considering the classification of people as targets and garbage while setting user profiles (Turow, 2011), demographic questions become more important.

Like recent studies (Benndorf & Normann, 2018; Winegar & Sunstein, 2019; Alfnes & Wasenden, 2022; Prince & Wallsten, 2022), we found that users exhibit a heterogeneous image in terms of willingness to sell their personal data for a certain reward. However, it is worth remembering again that the people who appear to have sold their personal data are users who can manipulate GOR to earn more rewards. We observed that the main problem likely to be experienced in transferring data to third-party ROPES as an intended use is the ambiguous attitude of users in answering the survey questions. Therefore, this is likely to pose a problem for the reliability of the data obtained by the ROPES.

In particular, the data regarding the trueness and certainty of the answers to the survey questions is a preliminary indicator of the complexity that can be encountered in displaying personalized advertisements and obtaining data for academic researches. Because GOR has not only been used for market research but also in many academic studies as a data collection tool (Sell, Goldberg & Conron, 2015; Harbach et al., 2016; Cornesse & Bosnjak, 2018; Ruktanonchai et al., 2018; Kanyadan & Ganti, 2019; Hogan et al., 2020). Participants in all these studies were rewarded with Google Play credits that they could spend in the Google Play Store. Considering that research on the coronavirus and other potential epidemic diseases can be carried out in the field of health in the future by targeting GOR users, it will once again become controversial over whether the data to be obtained is reliable owing to GOR users' application of masking as a counter-surveillance strategy.

Even if there appear to be no negative impacts on the surveillance mechanism's functionality (mobile apps are the very embodiment of this "surveillance mechanism"), the information obtained because of masking may be misleading or worthless, and it is likely that the authorities in charge of surveillance are not even aware of this (Marx, 2003). Therefore, in such mobile apps that may be developed in the future, the operation of a fairer and more reliable ecosystem in terms of voluntary data sharing by users will be developed. This will enable both the researchers who collect data and the users who will share their personal data to obtain a mutual benefit. In this context, while a privacy policy alone may

not be sufficient to address all consumer privacy concerns, it plays a crucial role in communicating with consumers and establishing accountability within an organization. By publicly disclosing its data practices, an organization can start to develop trust with consumers. Additionally, when a privacy policy is accessible through the app store, users can evaluate an app's privacy practices before deciding to download or buy it. Furthermore, a comprehensive privacy policy enables the FTC and State Attorneys General to enforce the commitments that apps make to consumers (Future of Privacy Forum, 2016).

The notion is believable that GOR users serve as app labourers who work for Google, handing over their personal data to its brand value and products recklessly in return for relatively low amounts of rewards. We are of the opinion that the most important cause for this is the more legal creation of surveillance in digital environments, and that the exploitation of "immaterial labor", which has been on the agenda in recent years, particularly in the digital area, is becoming more widespread.

CONCLUSIONS

The purpose of this article was to analyse the working mechanisms of the GOR mobile app, investigate the voluntary data sharing of app users, and to discover how the users utilize the app. The design of the GOR mobile app as a data storage application in return for a reward has been a reference for us in understanding the basic dynamics of mobile app users' sharing their data willingly in return for a reward.

Based on the basic working principles of GOR and the findings we obtained from the research results throughout the study, we determined that the data collected by mobile apps and shared willingly were used in academic research and market studies by third party ROPES researchers organisation paying for the e-survey. It can be argued that the use of GOR is a free action depending on the willpower of users. However, given that these data will be used to display personalized advertising to users or considering the purposes of use stated above, it is essential to conduct more comprehensive studies focusing on counter-surveillance strategies employed by users as well as mobile apps. There is amongst mobile apps an increasing manifestation of data abuse, not only because the attraction of winning awards is a driving force that directs the user to such apps, but also because it is challenging to decline to use these and similar technological products.

REFERENCES

Afolabi, O., Adeshola, I., Ozturen, A., and Ilkan, M. (2020). The influence of context on privacy concern in smart tourism destinations. *PEOPLE: International Journal of Social Sciences, 6*(1), 282–293.

Alfnes, F., & Wasenden, O. C. (2022). Your privacy for a discount? Exploring the willingness to share personal data for personalized offers. *Telecommunications Policy*, *46*(7), 1–10.

Arp, D., Quiring, E., Wressneger, C., and Rieck, K. 2017. Privacy threats through ultrasonic side channels on mobile devices. *IEEE European Symposium on Security and Privacy* (pp. 35–47).

Ataman, B., & Çoban, B. (2018). Counter-surveillance and alternative new media in Turkey. *Information, Communication & Society*, *21*(7), 1014–1029.

Barnes, S. (2006). A privacy paradox: social networking in the United States. doi:10.5210/fm.v11i9.1394

Bauer, C., & Strauss, C. (2016). Location-based advertising on mobile devices. *Management Review Quarterly, 66*(3), 159–194.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation.* John Wiley & Sons.

Benndorf, V., & Normann, H. T. (2018). The willingness to sell personal data. *The Scandinavian Journal of Economics*, *120*(4), 1260–1278.

Book, T., & Wallach, D. S. (2015). An empirical study of mobile ad targeting. Accessed 11 February 2021. https://arxiv.org/abs/1502.06577

Burton, F. (2007). The secerts of counter-survelliance. Strafor global intelligence. Accessed 20 February 2021. https://worldview.stratfor.com/article/secrets-countersurveillance

Carnegie Mellon University, (2020). Self-reported COVID-19 symptoms show promise for disease forecasts. Accessed 20 February 2021. https://www.cmu.edu/news/stories/archives/2020/april/self-reported-covid-19-symptoms-disease-forecasts.html

Castelluccia, C., Guerses, S., Hansen, M., Hoepman, Jaap-Henk., Hoboken, J., and Vieira, B. (2017). Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR Accessed 15 April 2021. https://pure.uva.nl/ws/files/42887337/22302384.pdf

Cecere, G., Le Guel, F., & Lefrere, V. (2020). Economics of free mobile apps: Personal data and third parties. Accessed 10 January 2021. https://ssrn.com/abstract=3136661

Cornesse, C., & Bosnjak, M. (2018). Is there an association between survey characteristics and representativeness? A meta-analysis. *Survey Research Methods, 12*(1), 1–13.

Dave, P. (2020). Google asks users about symptoms for Carnegie Mellon coronavirus forecasting effort. Accessed 10 February 2021. https://www.reuters.com/article/us-health-coronavirus-google-idUSKBN21B09Q

Demotriou, S., Merrill, W., Yang, W., Zhang, A., & Gunter, C. A. (2016). *Annual Network and Distributed System Security Symposium.* 1–15. Accessed 12 February 2021. http://youngwei.com/publication/pluto/

Donalek, J. G. (2004). Phenomenology as a qualitative research method. *Urologic Nursing*, *24*(6), 516–517.

Fernandes, E. R., & Oliveira, J. V. D. (2020). Quanto valem seus dados? O caso Google Opinion Rewards. *Revista de Direito e as Novas Tecnologias*, *7.*

Future of Privacy Forum, 2016. FPF mobile aaps study. Accessed 19 March 2021. https://fpf.org/wp-content/uploads/2016/08/2016-FPF-Mobile-Apps-Study_final.pdf

Gerber, N., Gerber, P., and Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security,* 77, 226–261.

Gibler, C., Crussell, J., Erickson, J., & Chen, H. (2012). Androidleaks: Automatically detecting potential privacy leaks in android applications on a large scale. In *Trust and Trustworthy Computing: 5th International Conference, TRUST 2012, Vienna, Austria, June 13–15, 2012. Proceedings 5* (pp. 291–307). Springer Berlin Heidelberg.

Google Play Store. (2020). Google Opinion Rewards. Accessed 20 February 2021. https://play.google.com/store/apps/details?id=com.google.android.apps.paidtasks&hl=tr&gl=US

Google Surveys Help. (2020). Targeting to Google Opinion Rewards. Accessed 01 February 2021.https://support.google.com/consumersurveys/answer/6013193?hl=en&ref_topic=6194671#zippy=%2Cdetermining-google-opinion-rewards-users-languages%2Cexpected-sampling-biases%2Cdifferences-by-country

Google Surveys Help. (2021). Types of questions. Accessed 01 February 2021. https://support.google.com/consumersurveys/answer/2446120?hl=en&ref_topic=6194671

Groenewald, T. (2004). A phenomenological research design illustrated. *International Journal of Qualitative Methods*, *3*(1), 42–55.

Gurria, A. (2008). Ministerial Meeting on the future of the internet economy. Accesed March 2021. https://www.oecd.org/fr/sti/closingremarksbyangelgurriaoecdministerialmeetingonthefutureoftheinterneteconomy.htm

Harbach, M., DeLuca, A., Malkin, N., & Egelman, S. (2016). Keep on lockin' in the free world: A multi-national comparison of smartphone locking. *CHI ,16: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems,* 4823–4827.

Ham, Chang-Dae. (2016). Exploring how consumers cope with online behavioral advertising. *Journal of Advertising, 36*(4), 632–658.

Han, M., Shen, S., Zhou, Y., Xu, Z., Miao, T., & Qi, J. (2019). An analysis of the cause of privacy paradox among SNS users: Take Chinese college students as an example.

Hogan, C., Atta, M., Anderson, P., Stead, T., Solomon, M., Banerjee, P., Sleigh, B., Shivdat, J., McAdams, A. W., & Ganti, L. (2020). Knowledge and attitudes of us adults regarding COVID-19. *International Journal of Emergency Medicine,* 53, 1–6.

Humby, C. (2006). Data is the new oil. Accessed 24 April 2021. http://ana.blogs.com/maestros/2006/11/data_is_the_new.html.

Hyrynsalmi, S., Suominen, A., Mäkilä, T., Järvi, A., & Knuutila, T. (2012). Revenue models of application developers in android market ecosystem. In *Software Business: Third International Conference, ICSOB 2012, Cambridge, MA, USA, June 18–20, 2012. Proceedings 3* (pp. 209–222). Springer Berlin Heidelberg.

Jorgensen, Z., Chen, J., Gates, C. S., Li, N., Proctor, R. W., & Yu, T. (2015). Dimensions of risk in mobile applications: A user study. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy* (pp. 49–60).

Jung, J., Shim, S. W., Jin, H. S., and Khang, H. (2015). Factors affecting attitudes and behavioral intention towards social networking advertising: A case of Facebook users in South Korea. *Journal of Advertising, 35*(2), 248–265.

Kadivar, J. (2015). Government Surveillance and Counter-Surveillance on Social and Mobile Media: The Case of Iran (2009). *M/C Journal*, *18*(2).

Kanyadan, V., & Ganti, L. (2019). E-cigarette awareness among young adults. *Palo Alto, 11*(7), 1–10.

Karafiloski, E., & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In *IEEE EUROCON 2017 – 17th International Conference on Smart Technologies* (pp. 763–768). IEEE.

Kokolakis, S. 2017. Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security,* 64, 122–134.

Kornstein, H. (2019). Under her eye: Digital drag as obfuscation and countersurveillance. *Surveillance & Society*, *17*(5), 681–698.

Lazzarato, M. (1996). Immaterial labor. Trans. P. Callili and E. Emory. In *Radical thought in Italy: A potential politics*, ed. M. Hardt and P. Virno. Minneapolis: University of Minnesota Press.

Leontiadis, I., Efstratiou, C., Picone, M., & Mascolo, C. (2012). Don't kill my ads! balancing privacy in an ad-supported mobile application market. In *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications* (pp. 1–6).

Lyon, D. (2001). *Surveillance society: Monitoring everyday life (Issues in society).* Open University Press.

Lyon, D. (2007). *Surveillance studies: An overview.* Cambridge: Polity Press.

Marx, G. T. (2003). A Tack in the shoe: Neutralizing and resisting. *Journal of Social Issues*, *59*(2), 369–390.

Meng, W., Ding, R., Chung, S. P., Han, S., & Lee, W. (2016). The price of free: privacy leakage in personalized mobile in-app ads. *Conference: Network and Distributed System Security Symposium,* (pp. 1–15).

Nath, S. (2015). Madscope: Characterizing mobile in-app targeted ads. *MobiSys ,15: Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services* May 2015, (pp. 59–73). doi:10.1145/2742647.2742653

Pew Research Center. (2021). Questionnaire design. Accessed 10 April 2021. https://www.pewresearch.org/methods/u-s-survey-research/questionnaire-design/

Polykalas, S. E., and Prezerakos, G. N. (2019). When the mobile app is freethe products is your personal data. *Digital Policy, Regulation and Government, 21*(2), 89–101.

Prince, J. T., & Wallsten, S. (2022). How much is privacy worth around the world and across platforms? *Journal of Economics & Management Strategy*, *31*(4), 841–861.

Qui, J. L. (2014). Goodbye iSlave: Foxconn, digital capitalism, and networked labor resistance. *Society: Chinese Journal of Sociology/Shehui*, *34*(4), 119–137.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., & Gill, P. (2018). Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. *The 25th Annual Network and Distributed System Security Symposium* 1–15. San Diego.

Ruktanonchai, N. W., Ruktanonchai, C. W., Floyd, J. R., & Tatem, A. J. (2018). Using Google location history data to quantify fine-scale human mobility. International. *Journal of Health Geographics, 17*(1), 1–13. doi:10.1186/s12942-018-0150-z

Sanchez, F. J. S., Aguado, J. M., and Martinez, I. (2019). Privacy paradox in the mobile environment: The influence of the emotions. *Professional de la Informacion, 28*(2), 1–11.

Sandelowski, M. (2000). Combining qualitative and quantitative sampling, data collection, and analysis techniques in mixed-method studies. *Research in nursing & health*, *23*(3), 246–255.

Segijn, C. E., Voorveld, H., and Vakeel, K. A. (2021). The role of ad sequence and privacy concerns in personalized advertising: An eye-tracking study into synced advertising effects. *Journal of Advertising, 50*(3), 320–329.

Sell, R., Goldberg, S., & Conron, K. (2015). The utility of an online convenience panel for reaching rare and dispersed populations. *PLoS ONE 10*(12), 1–10.

Shoaibi, D. A., & Rassan, I. A. (2012). Mobile advertising using location-based services. *2012 IEEE First International Conference on Internet Operating Systems.* doi:10.1109/icios.2012.15

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., and Borgthorsson, H. 2014. *Leakiness and creepiness in app space. Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems-CHI '14.* doi:10.1145/2556288.255742

Statista. (2021). Distribution of free and paid apps in the Apple App Store and Google Play as of Accessed 16 March 2021. https://www.statista.com/statistics/263797/number-of-applications-for-mobile-phones/

Taddicken, M. (2014). The 'privacy paradox' in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Comput-Med Commun, 19*(2), 248–273.

Tay, S. W., Teh, P. S., and Payne, S. J. (2021). Reasoning about privacy in mobile application install decisions: Risk perception and framing. *International Journal of Human-Computer Studies,* 145, 1–11.

Turow, J. (2011). T*he daily you: How the new advertising industry is defining your identity and your worth*. Yale University Press.

Ullah, I., Boreli, R., Kaafar, M. A., & Kanhere, S. S. (2014). Characterising user targeting for in-app mobile ads. *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* 547–552.

Wenz, A., Jäckle, A., and Couper, M. P. 2019. Willingness to use mobile technologies for data collection in a probability household panel. *Survery Research Methods, 13*(1), 1–22.

Wilson, D. (2012). Counter-Surveillance: Protest and Policing. *Plymouth Law and Criminal Justice Review,* 4, 33–42.

Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy*, *42*, 425–440.

Zhang, Y., Yang, M., Xu, B., Yang, Z., Gu, G., Ning, P., Wang, S. X., & Zang, B. (2013). Vetting undesirable behaviors in android apps with permission use analysis. *CCS ,13: Proceedings of the 2013 ACM SIGSAC Conference on Computer & communications security* (pp. 611–622).

Zhou, Y., Zhang, X., Jiang, X., & Freeh, V. W. (2011). Taming information-stealing smartphone applications (on android). In *Trust and Trustworthy Computing: 4th International Conference, TRUST 2011, Pittsburgh, PA, USA, June 22–24, 2011. Proceedings 4* (pp. 93–107). Springer Berlin Heidelberg.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019.* Profile books.