# Digital Surveillance Perception in Mobile Media Advertisements: A Comparison between Digital Generations<sup>1</sup>

#### Ömür TALAY

Akdeniz University

Institute of Social Sciences Department of Communication

Antalya

omurtalay@akdeniz.edu.tr

#### **Abstract**

With the transformation of individuals' lives by technological changes, the field of advertising has instrumentally and contextually transformed, digital communication applications have gradually spreaded to a broader mass and accordingly, and digital advertising has expanded its field of movement. The locating/positioning of digital environment and tools in individuals' lives in an irreplaceable way has led to the formation of a digital culture. Therefore, while the modern-day technology has been transforming the culture, digital surveillance systems has become digitalized, surveillance has changed into a cultural form and the digitalized surveillance has done the groundwork for the revealing of many cases of privacy violations in administrative and commercial domains. The digital prints left by the users while using the internet and the personal data leaked by the mobile applications are obtained and used by companies and advertisers in order to create the customer profile, and they also follow the users' interests in mobile environments, then serve advertisements to the users under the name of "personalization," and these lead to the ethical problems and privacy violations. The purpose of this study is the revealing of the intergenerational levels of users' awareness in regard to privacy violations and ethical problems caused by digital surveillance and the tracking of digital prints underlying the protection of privacy of lives', to mention the problems which may appear due to these differences with a scientific method and to propose solutions. In accordance with the purpose, the awareness, perceptions, the levels of concern about privacy of digital immigrants and digital natives are comparatively analysed and evaluated within the scope of the notion of surveillance in mobile environment advertisements by utilizing face to face survey method.

**Keywords:** Mobile Advertising, Digital Surveillance, Data Surveillance, Digital Immigrant, Digital Native.

# Mobil Ortam Reklamlarında Dijital Gözetim Algısı: Dijital Kuşaklar Arasında Bir Karşılaştırma

#### Özet

Teknolojik gelişmeler insan hayatını hızla dönüştürürken, reklamcılık alanı da araçsal ve içeriksel dönüşüme uğramış, dijital iletişim uygulamaları giderek geniş kitlelere yayılmış ve dijital reklam da buna bağlı olarak hareket alanını genişletmiştir. Dijital ortam ve araçların

<sup>&</sup>lt;sup>1</sup> This study is the abstract of the master's degree thesis called "Digital Surveillance Perception in Mobile Media Advertisements: A Comparison Between Digital Generations" presented at the institute of social sciences of Akdeniz University in 2018 under the supervision of Prof. Dr. Merih TAŞKAYA.

insan hayatında yeri doldurulamayacak bir biçimde konumlanması/konumlandırılması, dijital bir kültürün oluşmasını sağlamıştır. Böylece günümüz teknolojisi kültürü dönüştürürken gözetim sistemleri de dijitalleşmiş, gözetim kültürel bir forma bürünmüş, dijitalleşen gözetim yönetsel ve tecimsel alanlarda, mahremiyetin ihlal edildiği çok sayıda vakanın ortaya çıkmasının zeminini hazırlamıştır. Kullanıcıların internet kullanımı esnasında arkasında bıraktığı dijital izler ve mobil uygulamalarca sızdırılan kişisel verilerin şirketler ve reklam verenler tarafından elde edilmesiyle bu verileri müşteri profili oluşturmak için kullanmaları ya da kullanıcının mobil ortamlarda ilgilendiği konuları takip edilerek "kişiselleştirme" adı altında kullanıcılara reklam göstermeleri etik sorunları ve mahremiyet ihlallerini de beraberinde getirmektedir. Bu çalışmanın amacı özel hayatın gizliliğinin korunması temelinde, dijital gözetim ve dijital iz takibinin yol açacağı mahremiyet ihlallerinin ve etik sorunlara ilişkin kullanıcı farkındalığının kuşaklar arası düzeylerinin ortaya konulması, bu farklılıkların yol açabileceği problemlere bilimsel bir yöntemle işaret etmek ve çözüm önerileri sunmaktır. Bu amaç doğrultusunda dijital göçmen ve dijital yerlilerin dijital gözetime ilişkin farkındalıkları, algıları, gizlilik endişesi düzeyleri ve mobil ortam reklamlarında gözetim olgusu kapsamında yüz yüze anket tekniği ile elde edilen verilerden hareketle, karşılaştırmalı olarak analiz edilip değerlendirilmiştir.

**Anahtar Kelimeler:** Mobil Reklam, Dijital Gözetim, Veri Gözetimi, Dijital Göçmenler, Dijital Yerliler.

#### Introduction

While the gradual proliferation of surveillance under present conditions shed light on the digital surveillance notion, it also brings the question to what extent mobile technologies which surround many parts of daily life are used as control and surveillance mechanisms. Correspondingly, on the face of the mobile devices' evaluation which provides internet users' access to information as the platforms with which the user's digital tracks are followed, it is discussed that there are approaches suggesting network technologies are gradually transformed into surveillance systems. "Personalization", which is created either with the digital tracks left by the users on the internet or with the creation of customer profile by using personal data leaked by mobile applications and with the determination of profiles within the scope of the users' interests on mobile media, brings the ethical questions and concerns about the violation of privacy.

The skill of using digital communication channels and protection from the undesirable effects of digital communication channels is considered to be variable in accordance with users' conversancy situation with digital technology or users' condition of being born into these technologies. Generations, which vary in accordance with the articulation into digital culture or being born into digital culture, have needed to be identified once again when digital world has come into question. Marc Prensky has categorized the generations according to ages and technology uses in his works. He has divided these categories as the ones born

before 1980, the "Digital Immigrants" who met with technology afterwards and the ones born after 1980, the "Digital Natives" who are nested with technology (Prensky, 2001a, 2001b). Digital natives are born into technology and would not be devoid of technological devices. They can also use these devices in an effective way. On the other hand, digital immigrants are the ones who meet with technology afterwards, who try to understand and interpret the digital language, who have the ability to use technological devices but whose orientation period is longer when compared with digital natives.

"As the generations of sociologists are categorized as X, Y, Z; the opinion that this sectionalizing is done according to the interactivity of communication devices becomes strong" (Karahisar, 2013, p. 71). It is seen that this interaction is lower in X and Y generations than Z generation and Z generation chooses interactive digital media. At this point, it is important to scrutinize the differences among generation categories. For this, the suggestion of the differences between generations in their perceptions of surveillance will be useful.

The ethical problems caused by the personalization which is created by the determination of advertisement contents featured on mobile media within the scope of internet users' websites, search engines, mobile applications or their interests on social media and the problem that is determined within the scope of concerns regarding the violation of privacy are discussed in many extents. Although the awareness regarding the ethical violations and violations of privacy that can be created by the using of personal data obtained during/after personalization without individuals' consent or information shows difference between digital immigrants and digital natives, they stand in the same legal protection scope, and this is put forward as the research problem in our work.

The evaluation of the mobile devices, which helps internet users' access to information as the platforms through which user's digital tracks are followed, strengthens the arguments of the approaches towards network technologies' gradual transformation into surveillance systems. The aim of the research is to indicate privacy violations caused by digital surveillance and digital tracking, and to propose solutions via scientific methods. Meanwhile, the awareness regarding the ethical problems and the right of privacy would be discussed as well. In order to go through with this aim, the awareness and perceptions of digital immigrants and digital natives regarding digital surveillance and the ratings of the advertisements served at mobile media being watched, recognized and used are comparatively analyzed and evaluated within the context of surveillance phenomenon in mobile media advertisements.

The rapid evolvement of digitalization among society unveiled the notion of digital culture. The easy access of masses to information via internet-based mobile devices does not only attract individuals but also the companies, and apart from the information flow that they provide, this situation turns these devices into advertisement channels carried in the pockets. This situation has been conceptualized with the propositional phrase of "mobile media", and "mobile advertisements" started to give way to "internet-based mobile media advertisements" with the gradually developing mobile technology and mobile internet opportunities. In Turkish literature, a scientific work regarding the field work made upon the digital surveillance occurring during the usage of mobile communication media as an advertisement channel is not present. At this point, this work is important with its instructiveness and pioneering. Among the works done abroad, the works directly studying these subjects are limited. When the previous works are analyzed, it can be seen that, although the subjects such as surveillance in communication environments, surveillance in the internet and surveillance in social networks are touched upon; the perceptions and evaluations regarding the surveillance level at mobile media advertisements are disregarded. The information obtained within the scope of this work will serve to the development of perceptions and legal regulations regarding the ethical dimension of the applications in the field of informatics. This work will also contribute to the social sciences literature in a theoretical way.

Whether the individuals are aware of it or not, they are being tracked and controlled. This tracking and control occurs mainly via computer systems in the societies using information technologies. The surveillance at the communication environments has started to become so widespread that it almost became impossible in despite of the controlling of privacy violations, enforcements and legal regulations. Technology makes its presence felt at many points in daily lives and it provides convenience at daily use. But this situation does not change the fact that individuals give their personal data to the companies and states on a plate. Individuals' interests, religions, beliefs, behaviors and all activities are under digital custody and this information are used, controlled and directed with economic, social and cultural concerns. Along with the proliferation of surveillance in communication technologies, the scientific works regarding surveillance has become widespread and a study field called "surveillance works" emerged.

In French, the word "surveiller" means to watch, to monitor. "Surveillance is the collecting and processing of any identified or unidentified personal data with the aim of effecting or manipulating people whose data are collected" (Lyon, 2006, p. 13). Surveillance is the process that includes the monitoring of the information about individuals or companies

and the regulation, controlling, recording and categorizing of personal and social behaviors (Ball ve Webster, 2003; Hier ve Greenberg, 2007). The notion of surveillance exists since the emergence of social relations (Güven, 2011, p. 173). According to David Lyon (1997), surveillance is not a new thing. Since the immemorial, people have "looked" at the others in order to control things, to watch the process, to be organized or protect/defend. States, by recording and monitoring their citizens, want to make everything computable and readable (Arslantaş-Toktaş, Binark, Dikmen, Küzeci, Özaygen, 2012). According to William Bogard (1996), to monitor something is actually to monitor or protect it: For states, the easiest and the short-cut way of justifying surveillance is the terror precautions and protection discourses under the name of Bogard's notion of "protection."

From the literature of surveillance works, it can be seen that surveillance consists of chronologically three stages. The first stage starts with "Panoptic" period which has the structure that includes mostly architectural surveillance and discipline mechanisms. At the second stage, there is an evolvement from discipline to surveillance and control. This stage is the "Super-panoptic" period in which individuals are under ubiquitous surveillance that is based not on physical, but digital basis. In the third stage, "Data Surveillance" becomes prominent and this one is digital-based, constructed on the first two frames and at this stage, there are voluntary sharing, self-surveillance and monitoring among everyone. Today, the second and the third stages are the subjects of recent discussions.

From the main problem of the research, the work's theoretical frame is developed around Michel Foucault's "surveillance society" approach. Because the focus of the work is data surveillance, the problematic of the research is formulated with "digital surveillance" notion under the supervision of that approach. Lyon's claim that the collection and processing of data is made with the aim of "effecting and controlling individuals whose data are collected" strengthens the opinion that this work needs to be approached from this dimension. It has become impossible to evaluate today's society merely through Panopticon notion. The Panopticon notion brings light on Super-Panopticon and Synopticon notions (Öztürk, 2013, p. 133). Deleuze states that the disciplinarian power in modern capitalism is turning into a pattern in which individuals gradually adopt self-discipline without any external power and thus, societies are turning into a "self-control society" (quoted in Fuchs, 2015). Although surveillance is approached in terms of mostly discipline previously, today, with the developing technology and internet, this discipline mechanism has been turned into a consent-based character. Therefore the controlling has started to be seemed as flexible, the oppression created by the controlling has become invisible and the reaction of the supervised to the

supervisor has been weakened. All these became possible with the transformations created by the digitalization of controlling. The most important reason of that transformation, along with individuals' voluntary participation into surveillance, is to control bodies digitally and to make surveillance become an international controlling mechanism. Today, surveillance has transformed from architecture to technological devices with technological developments; digital surveillance has substituted architectural surveillance and this has started the period called "technological panopticon" or "post panopticon" (Çoban, 2016 p. 111).

## The Surveillance Phenomenon and the Economical Background in Digital Surveillance

Surveillance practices start with primitive tracking acts performed to make an impression suggesting that someone is taking care or examining another person (Lyon, 2013 p. 14, 15). In the old texts known as holy texts, it can be seen that surveillance is sometimes used as controlling and sometimes as taking care (Çakır, 2015, p. 195). Homes were thought to be the shelters that protect individuals from external violence or oppressions. But today, this thought is disrupted through the electronic devices and data transfer by individuals on purpose or unintendedly (Lyon, 2006, p. 37).

In the surveillance process, states or companies carry out the ways of data collection, storage, analysis, evaluation and usage with the aim of preventing specific groups' behaviors and in this process, physical, ideological or structural violence are potentially present and individuals are tried to be directed to particular behaviors. Digital surveillance does not make distinction between individuals and by controlling almost everyone, it creates a "mass surveillance" This the condition. situation removes distinction between suspicious/unsuspicious and makes everyone potentially suspicious. The leading motive of mass surveillance which is mostly unrecognized by the controlled ones gathers at three points: Protection, fight against terrorism and precautions for crimes (Cakır, 2015, pp. 248-317).

Personal data help modern states improve productivity and reach goals. The systems and devices developed for this brings together the effects that can make a change upon the whole society such as surveillance, control, discipline or guidance (Küzeci, 2010, p. 26). Because of that, the ruling power is in the need of knowing society more in order to control it (Karakehya, 2009, p. 334).

Although surveillance is mostly done by governments, recently major companies have become involved in the process of surveillance. The common connections of economical life such as production and consumption have become the subjects of surveillance. Surveillance is no more a disciplinary practice but it has leaked into the daily lives under the control of economical life with commercial concerns. Special profiles are created through individuals'

interests, production templates are designed according to these profiles and this situation is revealed via companies (Baştürk, 2016, p. 213). Individuals' habits are determined through Model of Living Analysis and profiles are determined according to these habits and behaviors. Model of living analysis is the method and computerized data collection that is used to document and understand the subject's habits, to detect the subject's previous behavior and present behaviors and to foresee the future behaviors.<sup>2</sup>

Surveillance systems gradually become less visible, more systematic and smarter (Lyon 2006, p. 12). The most important surveillance device is still the computers which enable the preserving, pairing, returning, processing and marketing of the data collected (Küzeci, 2010, p. 31). The developments in information technologies caused some transformations which were not present before in individuals' lives. Lives have been divided into two universes as "online" and "offline" and become bicentric (Bauman and Lyon, 2013, p. 51). It is widely accepted that in the online universe, surveillance is more intense, invisible and mostly made with consent.

## Mobility in Advertising and Digital Surveillance in Mobile Advertising

Advertising has started to be personalized and individualized as a result of the gradually increasing mobility and mobile devices being evaluated as a personal field. Mobile devices are easy to carry and accessible every time, they can be frequently used. The companies recognized the importance of reaching individuals upon the mobile media used on their mobile devices and mobile media advertising investments has increased. As mobile technologies develop, smart phones have become the products that take place in the daily lives of the users, leaving the characteristic of being an expensive interest behind. The functions performed by these devices are not only about making life easier, fun or socializing but also about reflecting and creating a self (Shklovski, Mainwaring, Skúladóttir, Borgthorsson, 2014).

Mobile devices have moved beyond from being a telephone to being a multifunctional device by taking the form of an interactive structure (Turow, 2015, p. 19). Interaction is one of the most important characteristics of communication technologies. Interaction is the enabling of the resource and receiver during communication and the occurring of these processes on the same communication channel (Başaran, 2010, p. 268). Along with the screens and interactive mobile communication integrated with media convergence, mobile devices have become mediums. This transformation has channeled the

\_

<sup>&</sup>lt;sup>2</sup> Joler et al. (2015)

interest towards traditional media into digital media; therefore media consumption patterns undergo a change in parallel with technological developments (Çaycı ve Karagülle, 2016, p. 573).

The mobility of individuals, the omnipresence of mobile devices and the opportunity of instant communication for users have resulted with advertisers effectively usage of "mobile advertisements". Mobile advertisements are the ones in which mobile-based advertisement messages are delivered to the individuals by publishers and advertisers. Besides, mobile advertising can be defined as the activity of advertising pursued upon mobile devices. Mobile advertising is mostly mentioned with interventions in freedom and violations of privacy. The concerns of protecting the consumers' personal data have arisen due to the mobile advertising's intrusiveness (Cleff, 2008, p. 423).

#### Personalization and Personalized Advertisements

Advertisers' focus has shifted from traditional mass advertising to personalized advertising because of the developments in mobile technologies. Personalized advertisements emerged from three consistent developments: Advertisers' desire of collecting personal data from users, the emergence of companies that can deliver these data as accessible and the development of technologies giving individuals the opportunity to choose advertisements (Turow, 2015, p. 138). Mobile devices' becoming personal fields have made personalized advertisements important for mobile environments. The activities of advertisements increase when the messages are sent as personalized instead of sending the same message to everyone. By means of user profiles, interest, brand preference and location based advertisements can be directed to a more essential target group. The measurements of advertisements in digital environments have become easier with the help of developed software and this situation has lowered errors.

Personalization can be defined as a communication strategy that includes the adding of the elements to the message based on the receiver's personal characteristics such as name, sex, location, occupation and previous behaviors that refers to each receiver (Maslowska, Smit, Van Den Putte, 2016). Customizability has turned into an ascending value in web environment. With identities and user habits becoming evident on web, appearances are made changeable according to the individual (Emiroğlu, 2009, p. 151). Personalization is not only used in web, but also in search engines, social media and mobile applications.

Personalized communication is thought to be an effective conviction strategy. It is verified that personalized advertising mediates the effects upon the attitudes towards attention, perception and message. Advertisements are personalized by including the user's

name and this personalization gets both negative and positive cognitive reactions (Maslowska et al, 2016).

#### Surveillance in Mobile Environments and Mobile Environment Advertisements

In online environments, almost all movements are tracked and recorded by hundreds of invisible followers, secret and silent "sensors" network whose existence are unknown that collects information about online movements.<sup>3</sup> Mobile environments, which are gradually being used commonly, have gained more places in daily lives and it has become inevitable to make works and processes at these environments (Sağıroğlu ve Mohammed, 2009, p. 146). Especially, with the superiority of Android operating system using mobile devices over Windows using mobile devices (both mobile and desktop) <sup>4</sup> and the supremacy of the usage level of mobile devices over desktop computer usage<sup>5</sup>; individuals have started to choose internet-connected mobile environments more and therefore, the advertisements published on these environments has considerably increased.

Internet-based mobile environments are gathered under four titles: web environment, search engines, social media and mobile applications. While the users are touring, searching on web environment or using a social media environment, they can access these environments either via a browser (which are actually mobile applications too) or a mobile application. Considering this, all of the environments above seem to be mobile application environments. However, because social media is an active and interactive environment and it has millions of users, it has to be evaluated as a primary environment. For instance, a flash light application which is only instantly helping users is not the same with Twitter on which millions of agendas is discussed. Also search engines have become a primary environment with high level of usage and indispensability (recently search engines can be accessed via widgets<sup>6</sup>).

Web environments, no matter with which device it is connected (whether via a browser or a mobile application or any widget), are the primary environments that exist since the emergence of internet and they underlie the surveillance on internet from the beginning. Also, because these environments have their own advertising ecosystem, it becomes difficult to evaluate them as separate environments. Dissimilarly from web, search engines and social media environments, mobile applications are the environments in which the present surveillance, digital tracking and personal data leaks are in highest gear. Today, various

<sup>&</sup>lt;sup>3</sup> Joler et al. (2015)

<sup>&</sup>lt;sup>4</sup> Android challanges. Windows as world's most popular operating system in terms of internet usage. (2017)

Mobile and tablet internet usage exceed desktop fort he first time worldwide. (2017)

<sup>&</sup>lt;sup>6</sup> Components of an application or interface that provide users access a service on mobile applications.

mobile applications on one hand make lives easier and on the other hand they do the groundwork for the collection of many personal data.

#### **Web Environment**

Web, which is one of the first applications of internet, can be considered as the starting point of digital surveillance within the scope of internet. The cookies, which are created especially for this field and which are used for digital tracking and profiling, are the most important surveillance mediums of this field.

Digital footprints, which are left behind by the users on digital services are being exploited with behavioral targeting and most part of the personal data are collected "without consent of the user". Digital footprints may include different kinds of information: these are sometimes IP addresses, web sites visited, the length and time of the visit, device type, search queries, location and sometimes sex and age, sexual preference or the books bought. When these information are gathered, they provide the creation of user profile, the occurrence of creation process and usage of the profiles that were created by computed data analysis and they also allow the discovery of patterns and relations inside of the data about users. Cookies decide and record the websites that the users visit, the advertisements they click and more importantly the products/services or subject that they have tendency to.

## **Search Engines**

In the early period, search engines were simply creating a word sequence regarding the document sequence including the searched words and they predicated this on the grading of whether that word is found in the texts or not (Dreyfus, 2016, p. 29). However, search engines do more than searching the desired words these days. Each word that is written on search engines are kept, individuals' profiles are created by categorizing these searches accepted as individuals' digital prints and personalized advertisements are delivered to users peculiar to these searches. Also, most of the advertisements that users encounter on web environment are obtained from these searches. A product/service that was searched on engines can be shown to users as strip advertisings on websites that have business partnership within a short time. On the other hand, some search engines may not prefer personalized advertisements (Adwords<sup>8</sup> etc.). The advertisements of products, services, web sites or various mobile applications are listed on top according to the searches user made.

Nowadays, keywords have gradually gained importance. One can get the desired results by merely writing a few words on search engines. These keywords are a service which

<sup>&</sup>lt;sup>7</sup> Passive digital footprint.

<sup>&</sup>lt;sup>8</sup> Google's advertising service.

is offered as a suggestion to the ones who give advertisements at Google's Adwords partnership program. By entering keywords about the product/service, one can get results closer to the target. All these characteristics of keywords play a key role for the surveillance in that environment. For instance, Google publishes the most searched words on Google search engine every year. As it can be understood, the product/service searches of users or their interests are obtained by the companies which own search engines and it works as a mechanism serving for the benefit of the companies.

### **Social Media**

Surveillance in social media is more detailed and extensive when compared with web and search engines. While browsing history and searched words come into prominence in web environment and search engines; social media includes all of these and extends its surveillance capacity because it has more detailed information about the users.

"Social media's existence depends on the tracking the users and selling the acquired information to others" (Bauman ve Lyon, 2013, p. 18). "More than three fourths of a billion people uploaded the most confidential things on Facebook within the five years after its formation" (Chatfield, 2013, p. 30). Social media usage is indigenized by daily life practices. This situation turned surveillance into a hyper-control. Social media companies' constant redirection to share personal information and images and their notices to make people share stories or statuses have the characteristics of participation invitation to exposal, surveillance and peeping (Çakır, 2015, pp. 332-374).

Social network sites are particularly accordant with targeted advertising because high amount of user likes and dislikes are stored and transmitted. Therefore, it becomes possible to control these data with economical aims and to find to which product users tend to buy. This situation defines the reason why targeted advertising is the main resource and business model of mostly profit-oriented social network sites. Facebook uses mass surveillance; it stores, compares, easily access and sell millions of different personal data (Fuchs, 2011, p. 138-139).

Although Facebook claims that it provides more privacy opportunities to its users than many other network sites, Facebook's ecosystem creates a communication pattern towards seeing, showing and surveillance (Korkmaz, 2013, p. 120). Also, the argument that it provides more privacy opportunities to its users has been destroyed with the personal data leaked to Cambridge Analytica. <sup>10</sup> Because the stories, personal data, photographs or comments are used by companies or shared with other companies and advertisers and individuals are not

<sup>&</sup>lt;sup>9</sup> İşte 2017'de Google'da en çok arananlar. (2018)

<sup>&</sup>lt;sup>10</sup> Bilmeniz gerekenler: Cambridge Analytica hikâyesi, Facebook ve büyük veri. (2018)

given commitments about the protection of these information; the privacy and confidentiality violations are claimed to continue to be on the agenda.

## **Mobile Applications**

Surveillance, digital tracking and personal data leaks are in high gear in mobile applications nowadays. Active usage of mobile devices increases the interest towards mobile applications and in parallel with this; it creates a good environment for the advertisements.

In-app advertising is a basic part of free mobile application ecosystem. This situation creates a "win-win gain" through which application developers gain favor without setting cost for the users. However, as it is the same in advertising on web environment, the advertising networks behind in-app advertising use personalization in order to develop the effectiveness/profitability of ad-placing. Advertising networks that need to offer personalized advertisements are urged to collect data about users and to create their profiles. But mobile application developers can create income with the help of in-app advertising by publishing their works freely. As it is in traditional web advertising, personalization develops the effectiveness of in-app advertising (and therefore, it increases the income of application developers). This kind of personalization occurs only when the advertiser can access to specific user information (for instance; interests, demographic information) and because of that, data leakage always become a problem (Meng, Ding, Chung, Han, Lee, 2016).

In a survey with 5000 mobile users made by Ipsos Otx<sup>11</sup> on April 2010 in USA, 82% of the participants stated that they realized the advertisements on smart phones and 49% of the participants stated that they took action depending on these advertisements. The advertisements in applications have an effect on users and their buying patterns. In 2012, global mobile advertising market was valued at approximately 5,3 million dollars and this shows the value of the access of advertisers to user patterns and personal data is.<sup>12</sup>

On primary platforms like Android, because most users log into their Google accounts before using the device, more personal data can be collected from these accounts. An advertising network can use these personal characteristics and offer in-app personalized advertisements to the targeted users in order to create/update user profiles with all potential ways of obtaining information. In-app advertising targets the advertisements published on the same authorization level with applications. Application developers can learn the users' real interests and demographic information by accessing to users' personalized advertisements in

\_

<sup>&</sup>lt;sup>11</sup> Binark et al. (2015)

<sup>&</sup>lt;sup>12</sup> Research into user perspectives on mobile privacy: Key findings from UK, Spain and Singapore. (2018, 17 May) Access address: <a href="https://www.gsma.com/publicpolicy/user-perspectives-on-mobile-privacy-september-2011">https://www.gsma.com/publicpolicy/user-perspectives-on-mobile-privacy-september-2011</a>

the application (Meng et al, 2016). Sometimes users are offered easy registration opportunity integrated with some major companies during the registration process after accessing the application. For instance, when logging into a mobile application, "Connect with Facebook" or "Continue with Google+" options are offered except for e-mail and password. This situation generally mentions the partnership of these companies.

Conducted researches show that there is a possibility of users' sensitive personal information to leak into third party application developers via personalized advertisements served in mobile application (Meng et al, 2016). From a different viewpoint, "data leakage" may be a misattribution – data flows provided by the application are not generally coincidental negligence or unmeant results; but they are the center of the business model that makes the application possible in the first place. "Intentional data distribution" is a more proper term (Shklovski et al., 2014). It can be concluded that mobile applications are main mechanisms for data leakage and data distribution is made consciously.

## **Research Methodology**

Face to face survey method is quantitatively used in this research. Because two groups were to be compared, participants' number was needed to be above 384 equally and the number of the conducted surveys was 832. As for digital immigrants, 412 survey results were obtained by making face to face interview. As for digital natives, 420 survey results were obtained by making face to face interview and in order to equalize this number with the result of digital immigrants, 412 of them were evaluated and 824 surveys were included in the research. During the research, participants were asked about their mobile internet usage and whether they use social media or not and face to face survey practice continued with the ones who use social media. The number of individuals who do not use mobile internet and social media is minute amount.

The research was conducted in three major counties<sup>13</sup> of the province of Ankara. Ankara was chosen mainly because it has a metropolitan and cosmopolitan characteristic and besides, it is the capital, there is an outgrowth of pensioner population<sup>14</sup> and public officers'<sup>15</sup> population, and there is an intimacy towards public institutes related with technology and informatics. Because there is an intergenerational evaluation in this work, the age of meeting with digital technology is important within the scope of the research.

<sup>&</sup>lt;sup>13</sup> Ankara ilçeleri nüfusu. (2018, 25 May) Access address: <a href="https://www.nufusu.com/ilceleri/ankara-ilceleri-nufusu">https://www.nufusu.com/ilceleri/ankara-ilceleri-nufusu</a>

<sup>&</sup>lt;sup>14</sup> Türkiye'nin emekli haritası çıkartıldı. (2018, 25 May) Access address: <a href="http://www.haberturk.com/ekonomi/is-yasam/haber/1544055-turkiye-nin-emekli-haritasi-cikartildi">http://www.haberturk.com/ekonomi/is-yasam/haber/1544055-turkiye-nin-emekli-haritasi-cikartildi</a>

<sup>&</sup>lt;sup>15</sup> Hangi şehirde kaç memur yaşıyor? (2018, 25 May) Access address: <a href="http://trend.mynet.com/hangi-sehirde-kac-memur-yasiyor-1036012">http://trend.mynet.com/hangi-sehirde-kac-memur-yasiyor-1036012</a>

The population comprises of individuals living in three major counties of the province of Ankara. The sample of the research comprises of individuals who use mobile devices and access internet via these devices whose ages are between 18 and 72. In the context of the research, there is digital surveillance occurring merely on mobile environment advertisements. The ones who connect to internet with non-mobile environments and the advertisements in non-mobile environments are excluded. The participants of the research are limited with 18-72 age range. The age of 18 was defined as the sublimit because this age did not require the permission of parents. The upper limit was defined as the people born between 1946 and 1964, called as "Baby Boomers" Quota sampling was chosen in the research; participants were divided into two groups as digital natives of ages 18-37 and digital natives of ages 38-72. Because of the ampleness of the sample, p and q values are taken as 0,05 and the 5% error margin was accepted as  $\alpha = 0,05$  and it was calculated as 384.

### **Findings**

## **Findings about Mobile Internet Access**

According to the findings that show participants' mobile internet access, access to the mobile internet via mobile phone took place on the top with 85,7% rate. As it can be seen, participants highly use mobile phones and mobile phone is followed respectively by luggable computer with 9,5% and tablet/ipad with 3,4% rate.

## Findings about the Use of Social Media Environment

At the use of social media, it is seen that two social media environments are used more. 44% of the participants use Instagram and 28,5% of them use Facebook. Then there comes respectively Twitter, Google+ and Whatsapp. In accordance with this finding, it can be predicted that individuals spend much time on social media and they use these environments intensively.

# Findings about the Awareness Stage of the Advertisements Published on Mobile Environments

92,8% of the participants stated that they realized the advertisements about the previously significant products/services which were published on mobile environments later on. 6,4% of the participants stated that they did not see advertisements on mobile environments. Therefore, it is shown that there is a high rate of these advertisements being realized.

Participants see advertisements on social media environment with a rate of 67,7%. After social media, there comes the search engines with a rate of 13,2%.

<sup>16</sup>https://www.academia.edu/19706219/Dijital\_Ku%C5%9Faklar\_Dijital\_Ku%C5%9Faklar%C4%B1\_Nas%C4%B1\_%C3%87al%C4%B1%C5%9Fmal%C4%B1?auto=download (Access date: 20.05.2018).

### Findings about the Concern Levels in Privacy and Confidentiality Violations

**Table 1.** The Distribution of the Findings Related to the Privacy Concerns Caused by the Situation of Seeing the Advertisement of Previously Searched Products/Services on Mobile Environments in Accordance with Generations

		Generation			
Answers related to privacy concerns		<b>Immigrant</b>	Native	Total	
Yes	N	332	252	584	
	%	<b>%81,0</b>	%61,5	%71,2	
No	N	78	158	236	
	%	%19,0	%38,5	%28,8	
Total	N	410	410	820	
	%	%100,0	%100,0	%100,0	

When the privacy violation concerns are analyzed according to the generations, striking result emerge. According to the findings, 81% of digital immigrants reported privacy violation concerns. As for the digital natives, the scale is narrow and the rate of the participants who reported privacy concerns is 61,5%. It can be concluded that digital immigrants, when compared with digital natives, have more concerns about privacy violation and they are scared from the violation of privacy more.

Table 2. The Concern Levels on Personalization-Privacy Violations

				The Concern Leve		
			Personalization	on Privacy Violation		
Spearman's rho	Personalization	Correlation	1,000	,302**		
		Coefficient				
		Sig. (2-tailed)		,000		
		N	817	804		
	The Concern	Correlation	,302**	1,000		
	Level on Privacy	Coefficient				
	Violation	Sig. (2-tailed)	,000			
		N	804	811		

<sup>\*\*.</sup> Correlation is significant at the 0.01 level (2-tailed).

As seen at Table 2, the significancy value of correlation is measured as ',302\*\*' and a positive relation is in question. Therefore, the personalization used in mobile environment advertisements increases the concern related to the violation of privacy in the context of digital surveillance.

**Table 3.** The Levels of Concern About Privacy

Privacy Concern

Mann-Whitney U	67650,000	
Wilcoxon W	151905,000	
Z	-6,167	
Asymp. Sig. (2-tailed)	,000	

As seen at Table 3, the Asymp. Sig. (2-tailed) value is measured as ',000' and because this value is lower than '0,05', there is a significant difference between the levels of concern of digital immigrants and digital natives as a result of the exposition to the advertisements related to the products and services they searched for.

## Findings about the Awareness Regarding Digital Surveillance

**Table 4.** Digital Surveillance Awareness on Mobile Environments According to Generations

The answers of participants regarding the question whether they are aware of the digital surveillance			Gener		
on mobile environments or not	<b>9</b> ··· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·		Immigrant	Native	Total
	Agree	N	314	271	585
		%	%78,3	<b>%67,1</b>	%72,7
	Neutral	N	42	61	103
		%	%10,5	%15,1	%12,8
	Do not agree	N	29	61	90
		%	%7,2	%15,1	%11,2
	Do not know	N	16	11	27
		%	%4,0	%2,7	%3,4
	Total	N	401	404	805
		%	%100,0	%100,0	%100,0

According to the findings, 78,3% of digital immigrants and 67,1 of digital natives are aware of the surveillance on mobile environment advertising. 72,7% of total participants are aware, 12,8% of them are neutral and slightly (11,2%) they are not aware. 3,4% of the participants stated that they do not know. As a result, both digital immigrants and digital natives have the feeling that they are being tracked on mobile environments.

**Table 5.** The Recognition Stage of the Possibility of Mobile Applications Sharing Users' Personal Information with Third Parties According to the Generations

	Generation					
The answers of the participants regarding personal information sharing on mobile environments Immigrant Native T						
Agree	N	245	244	489		
	%	%60,3	<b>%60,4</b>	%60,4		
Neutral	N	53	75	128		
	%	%13,1	%18,6	%15,8		
Do not ag	gree N	43	54	97		
	%	%10,6	%13,4	%12,0		

	o not know N	65	21	96
D			0/7.7	
	%		%7,7	%11,9
To	otal N	406	404	810
	%	%100,0	%100,0	%100,0

According to the findings towards measuring the awareness regarding the possibility of mobile applications sharing users' personal information with third parties, both groups showed approximately 60% awareness. However, the answer as "do not know" of digital immigrants with a rate of 16% is higher than digital natives' (7,7%) and it is understood that digital natives are more grasped than digital immigrants. From the rates of neutrals, it can be seen that digital natives are more indecisive than digital immigrants.

**Table 6.** The Status of Being Informed about Cookies According to Generations

			0		
			Gener	ation	
Answers regarding the recognition	Answers regarding the recognition of cookies		<b>Immigrant</b>	Native	Total
	Agree	N	91	153	244
		%	%22,4	%37,5	%30,0
	Neutral	N	51	93	144
		%	%12,6	%22,8	%17,7
	Do not agree	N	53	72	125
		%	%13,1	%17,6	%15,4
	Do not know	N	211	90	301
		%	%52,0	%22,1	%37,0
Total		N	406	408	814
		%	%100,0	%100,0	%100,0

The findings show that the recognition of cookies which are used for digital surveillance on web environment was questioned and it is seen that digital immigrants have very few information. 52% of the digital immigrants do not have information about cookies and 37,5% of digital natives have information. Generally, there is a lack of knowledge (37%) about the cookies. Cookies are arranged openly in a standard way on web sites or mobile-based applications. When users download the application or use a web service, they automatically allow cookies. Unless they change this option from the software settings, cookies continue recording data. This situation causes data to be recorded without informing the user and it also causes the violation of privacy and confidentiality. The fact that companies, web sites or mobile applications do not inform users enough is among the findings.

#### **Conclusion**

The surveillance of individuals has become easier and widespread with the help of various applications and therefore, it has justified surveillance on the internet more. The effort of "tracking the daily life" which was mentioned by David Lyon (2006) has resulted with the

tracking of almost all activities of individuals and thus, surveillance which is continuous and functional for the observer has gradually become widespread. As Michel Foucault (1992) stated, "always keeping a close watch" has gradually passed through individuals and it has affected the daily life. Such that, except for the companies and states, individuals have started to observe each other secretly and they have participated into surveillance.

Surveillance happening on mobile environment advertisements is made via "personalization" and it causes personal data to be used without consent of individuals. Privacy and confidentiality violations on mobile environments have increased recently and these environments have become the center of data leakage that is made through mobile devices accepted as the personal field of users. Under the light of the observations made on the field and digital environment during research and the findings, it is understood that surveillance on mobile environments occurs as a result of the effort of obtaining personal data for personalization. The situation that happens when an advertisement appears about the previously searched product/services (for instance, when air-conditioner is searched on any engine, it appears as strip advertising on web or advertisements including product's features and even prices appears on social media or other mobile environments) reveals this fact. Related literature supports this result too. According to the findings, digital immigrants are more concerned about the confidentiality violations caused by mobile environment surveillance, therefore, their awareness of surveillance are more. Digital natives' ability of dealing with surveillance is higher than digital immigrants' and this can explain their awareness' being low.

Although the digital immigrants' awareness of digital surveillance is high, they are less informed of technology and applications than digital natives. Digital immigrants are also more concerned about confidentiality violation than digital natives. Moreover, digital immigrants have less hope than digital natives about the protection of confidentiality. Thus, the idea of protection's impossibility has become stereotyped and individuals do not question surveillance.

The reaction of individuals to surveillance is mostly being neutral. The ones who are aware of surveillance do not react to it and think that s/he will not be affected from it. Also, individuals think that surveillance was always present and it will continue to be and they accept it. This situation points to the term Panopticon and shows that surveillance is an activity that creates learned helplessness. When data leakage is taken into consideration, whether individuals share personal information or not, these information are leaked to the third parties. Also, it is seen that the price of free applications, which are thought to be used

freely, is the losing of personal and confidential information. Likewise, the permissions given without reading cookie and privacy policies give way to personal data's becoming open to companies and advertisers.

Individuals especially ignore the notice about cookie policies on websites. Even if they do not, these policies are long and incomprehensible. Therefore, these policies should be regulated by considering the intergenerational differences.

As for the access permission which is the most important medium of data leakage in mobile applications, although individuals give attention to these permissions, they do not give up using that application. Therefore, it is understood that individuals' use or nonuse of the mobile application depending on its access permissions is important for the works in the mobile fields. More sensitive protection needs to be created upon the more and demography-based digital separation in order to create a defense against privacy violations in in-app personalized advertisements (Meng et al, 2016).

It is understood that the responsibility of protecting from digital surveillance happening via the advertisements published on mobile environments is given to individuals/users within the frame of related legal regulations. Therefore, more importance must be given to media literacy. Also, in order to have the ability to read advertisements in a critical way, the general education structure, thus the curriculum towards media literacy, needs to be prepared and used with a critical perspective (Taşkaya, 2016, p. 227).

It is discussed in the work that, although the recognition of digital surveillance varies from digital immigrants to digital natives, it takes part on the same legal protection frame and it was revealed that the regulations about the protection of personal data and consumer needs to be organized by taking the generations age, education status, digital opportunities and digital skills into consideration – especially within the scope of penal sanctions. At this point, it seems impossible to protect oneself from surveillance's effects and to protect privacy on a personal level. It is not a remote possibility that the most important human rights violations that can happen in the future will be by means of the opportunities and order that this system provided and justified (Yanık, 2017, p. 796). So, current legal regulations and laws should be revised according to the intergenerational perception and awareness levels on digital surveillance. The results obtained within this research would be crucial and useful for the forthcoming researches.

#### References

- Arslantaş-Toktaş, S., Binark, M., Dikmen, E. Ş., Küzeci, E., & Özaygen, A. (2012).

  Türkiye'de dijital gözetim: Tc. kimlik kartlarından e-kimlik kartlarına yurttaşın sayısal bedenlenişi. İstanbul: Alternatif Bilişim Derneği.
- Ball, K. & Webster, F. (2003). *The intensification of surveillance. crime, terrorism and warfare in the information age.* London: Pluto Press.
- Başaran, F. (2010). Yeni iletişim teknolojileri, alternatif iletişim olanakları. *Mülkiye Dergisi*, *34*(269). pp. 255-270, retrieved 24.7.2017, from http://mulkiyedergi.org/
- Baştürk, E. (2016) Gözetimin soykütüğü: Foucault'dan Deleuze'e postmodern bir arkeoloji. İstanbul: Kalkedon Yayıncılık.
- Bauman, Z. & Lyon, D. (2013). *Akışkan gözetim*. (E. Yılmaz, Çev.). İstanbul: Ayrıntı Yayınları.
- Bogard, W. (1996). *The simulation of surveillance: hypercontrol in telematic societies*. London: Cambridge University Press.
- Chatfield, T. (2013). *Dijital çağa nasıl uyum sağlarız*. (L. Konca, Çev.). İstanbul: Sel Yayıncılık.
- Cleff, E. B. (2008). Regulating mobile advertising in the European Union and the United States. *Computer Law & Security Review*, 24(5), pp. 421-436, retrieved 5.5.2017, from https://www.sciencedirect.com/
- Çakır, M. (2015). İnternette gösteri ve gözetim. eleştirel bir okuma. Ankara: Ütopya Yayınevi.
- Çaycı, B. & Karagülle, A. E. (2016). İletişimin dijitalleşmesi ve kültürel melezleşme. *Global Media Journal: Turkish Edition*, *6*(12), pp. 570-586, retrieved 8.10.2017, from http://globalmediajournaltr.yeditepe.edu.tr/
- Çoban, B. (2016). Gözün iktidarı üzerine, B. Çoban ve Z. Özarslan (Çev. hzl.). *Panoptikon: Gözün iktidarı* içinde. (s. 111-138). İstanbul: Su Yayınları.
- Dreyfus H. L. (2016). İnternet Üzerine. (V.M. Demir, Çev.). İstanbul: Küre Yayınları.
- Emiroğlu, B.G. (2009, Şubat). *Semantik web (anlamsal ağ) yapıları ve yansımaları*. XI. Akademik Bilişim Konferansı'nda sunulan bildiri. Harran Üniversitesi, Şanlıurfa, retrieved 3.11.2017, from http://ab.org.tr/
- Foucault, M. (1992). Hapishanenin Doğuşu. (M. A. Kılıçbay, Çev.). Ankara: İmge Kitabevi.
- Fuchs, C. (2011). New media, web 2.0 and surveillance. *Sociology Compass*, *5*(2), pp. 134-147, retrieved 1.2.2016, from doi: 10.1111/j.1751-9020.2010.00354.x

- Fuchs, C. (2015). *Dijital emek ve Karl Marx*. (T. E. Kalaycı ve S. Oğuz, Çev.). İstanbul: Nota Bene Yayınları.
- Güven, S. K. (2011). Gözetimin toplumsal meşruiyeti. H, Köse, (Ed.). *Medya mahrem & medyada mahremiyet olgusu ve transparan bir yaşamdan parçalar* içinde. (pp. 173-198.). İstanbul: Ayrıntı Yayınları.
- Hier, S. & Greenberg, J. (2007). The Surveillance Studies Reader. McGraw-Hill Education.
- Karakehya, H. (2009). Gözetim ve suçla mücadele: Gözetimin tarihsel gelişimi ile yakın dönemde gerçekleştirilen hukuki düzenleme ve uygulamalar bağlamında bir değerlendirme. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, *58*(2), pp. 319-357, retrieved 2.10.2016, from http://dergiler.ankara.edu.tr/
- Karahisar, T. (2013). Dijital nesil, *dijital iletişim ve dijitalleşen* (!) Türkçe. *AJIT-e: Online Academic Journal of Information Technology, 4*(12), pp. 71-83, retrieved 29.4.2017, from http://www.acarindex.com/
- Küzeci, E. (2010). Kişisel verilerin korunması. Ankara: Turhan Kitabevi.
- Korkmaz, İ. (2013). Facebook ve mahremiyet: görmek ve gözetle(n)mek. *Yalova Üniversitesi Sosyal Bilimler Dergisi*, *3*(5), pp. 107-122, retrieved 3.1.2017, from http://yusbed.yalova.edu.tr/
- Lyon, D. (1997). *Elektronik göz*. (D. Hattatoğlu, Çev.). İstanbul: Sarmal Yayınevi.
- Lyon, D. (2006). *Gözetlenen toplum: Günlük hayatı kontrol etmek.* (G. Soykan, Çev.). İstanbul: Kalkedon Yayıncılık,
- Lyon, D. (2013). Gözetim çalışmaları. (A. Toprak, Çev.). İstanbul: Kalkedon Yayıncılık.
- Maslowska, E., Smit, E. G. & Van Den Putte, B. (2016). It is all in the name: A study of consumers' responses to personalized communication. *Journal of Interactive Advertising*, 16(1), pp. 74-85, retrieved 9.12.2017, from doi: 10.1080/15252019.2016.1161568
- Meng, W. Ding R., Chung S. P., Han S., & Lee W. (2016:) The price of free: Privacy leakage in personalized mobile in-apps ads. *23nd Annual Network and Distributed System Security Symposium*. pp. 1-15, retrieved 1.11.2017, from 10.14722/ndss.2016.23353
- Öztürk, S. (2013). Filmlerle görünürlüğün dönüşümü: Panoptikon, süperpanoptikon, sinoptikon. *İletişim Kuram ve Araştırma Dergisi*, (36), pp. 132-151, retrieved 2.2.2016, from <a href="http://iletisimdergisi.gazi.edu.tr/">http://iletisimdergisi.gazi.edu.tr/</a>
- Prensky, M. (2001a). Digital natives, digital immigrants. On the Horizon 9(5), pp. 1-6, retrieved 18.10.2016,

- from https://www.marcprensky.com/writing/Prensky%20%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf
- Prensky, M. (2001b). *Digital natives, digital immigrants, part II: do they really think differently? On the Horizon 9*(6), pp. 1-6, retrieved 18.10.2016, from <a href="http://d.scribd.com/docs/25yfw2gwramobinjk3vt.pdf">http://d.scribd.com/docs/25yfw2gwramobinjk3vt.pdf</a>
- Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. pp. 2347-2356, retrieved 8.3.2016, from doi: 10.1145/2556288.2557421
- Sağıroğlu Ş. & Mohammed M. (2009). Mobil ortamlara yapılan saldırılar üzerine bir inceleme. *Tübav Bilim Dergisi 2*(2), pp. 138-147, retrieved 5.9.2017, from http://dergipark.gov.tr/
- Taşkaya, M. (2016). Eleştirel Reklam Okuryazarlığı. E. Küçük Durur (Ed.). *Medya Okuryazarlığı* içinde. (s. 189-230). Ankara: Siyasal Kitabevi.
- Tonta, Y. (2009). Dijital yerliler, sosyal ağlar ve kütüphanelerin geleceği. *Türk Kütüphaneciliği*, 23(4), pp. 742-768, retrieved 16.6.2016, from http://www.tk.org.tr/

  Turow, J. (2015). *İzleniyoruz*. (M. Benveniste, Çev.). İstanbul: Hil Yayın.
- Yanık, A. (2017). Bir süperpanoptikon olarak yeni medya: Yeni medya ışığında gözetimin eleştirisi. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, *5*(2), pp. 784-800, retrieved 3.5.2018, from http://dergipark.gov.tr/

#### **Internet Resources**

- Joler et al. (2015) Metadata Investigation: Inside Hacking Team. Retrieved on December 15<sup>th</sup> 2017 from <a href="http://gs.statcounter.com/press/android-challenges-windows-as-worlds-most-popular-operating-system">http://gs.statcounter.com/press/android-challenges-windows-as-worlds-most-popular-operating-system</a>
- Mobile and tablet internet usage exceeds desktop for first time worldwide, retrieved 13.09.2018, from <a href="http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide">http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide</a>
- İşte 2017'de Google'da en çok arananlar, retrieved 18.05.2018, from http://t24.com.tr/haber/iste-2017de-googleda-en-cok-arananlar,525250
- Bilmeniz gerekenler: Cambridge Analytica hikayesi, Facebook ve büyük veri, retrieved 22.03.2018, from <a href="https://webrazzi.com/2018/03/22/cambridge-analytica-hikayesi-facebook-ve-buyuk-veri">https://webrazzi.com/2018/03/22/cambridge-analytica-hikayesi-facebook-ve-buyuk-veri</a>

The mobile movement. retrieved 17.05.2018, from

https://www.thinkwithgoogle.com/advertising-channels/mobile/the-mobile-movement/

Research into user perspectives on mobile privacy: Key findings from UK, Spain and Singapore, retrieved 17.05.2018, from <a href="https://www.gsma.com/publicpolicy/user-perspectives-on-mobile-privacy-september-2011">https://www.gsma.com/publicpolicy/user-perspectives-on-mobile-privacy-september-2011</a>

Ankara ilçeleri nüfusu, retrieved 25.05.2018, from <a href="https://www.nufusu.com/ilceleri/ankara-ilceleri-nufusu">https://www.nufusu.com/ilceleri/ankara-ilceleri-nufusu</a>

Türkiye'nin emekli haritası çıkartıldı, retrieved 25.05.2018, from
<a href="http://www.haberturk.com/ekonomi/is-yasam/haber/1544055-turkiye-nin-emekli-haritasi-cikartildi">http://www.haberturk.com/ekonomi/is-yasam/haber/1544055-turkiye-nin-emekli-haritasi-cikartildi</a>

Hangi şehirde kaç memur yaşıyor? retrieved 25.05.2018, from <a href="http://trend.mynet.com/hangi-sehirde-kac-memur-yasiyor-1036012">http://trend.mynet.com/hangi-sehirde-kac-memur-yasiyor-1036012</a>