ISCTE IUL
REPOSITÓRIO
INSTITUTO UNIVERSITÁRIO DE LISBOA

Repositório ISCTE-IUL

Deposited in *Repositório ISCTE-IUL*:
2019-01-07

Deposited version:
Post-print

Peer-review status of attached file:
Peer-reviewed

Citation for published item:
Rodrigues, N. & Oliveira, A. (2018). Remember when, on the internet, nobody knew who you were?. In Luis Gómez Chova; Agustín López Martínez; Ignacio Candel Torres (Ed.), 11th annual International Conference of Education, Research and Innovation, ICERI2018. (pp. 3871-3877). Seville: IATED Academy.

Further information on publisher's website:
10.21125/iceri.2018.1864

Publisher's copyright statement:
This is the peer reviewed version of the following article: Rodrigues, N. & Oliveira, A. (2018). Remember when, on the internet, nobody knew who you were?. In Luis Gómez Chova; Agustín López Martínez; Ignacio Candel Torres (Ed.), 11th annual International Conference of Education, Research and Innovation, ICERI2018. (pp. 3871-3877). Seville: IATED Academy., which has been published in final form at https://dx.doi.org/10.21125/iceri.2018.1864. This article may be used for non-commercial purposes in accordance with the Publisher's Terms and Conditions for self-archiving.

Use policy

Creative Commons CC BY 4.0
The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a link is made to the metadata record in the Repository
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Serviços de Informação e Documentação, Instituto Universitário de Lisboa (ISCTE-IUL)
Av. das Forças Armadas, Edifício II, 1649-026 Lisboa Portugal
Phone: +(351) 217 903 024 | e-mail: administrador.repositorio@iscte-iul.pt
https://repositorio.iscte-iul.pt

REMEMBER WHEN, ON THE INTERNET, NOBODY KNEW WHO YOU WERE?

Nelson Rodrigues[1], Abílio Oliveira[2]

[1]Instituto Universitário de Lisboa (ISCTE-IUL) (PORTUGAL)
[2]Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR-IUL, Lisboa (PORTUGAL)

Abstract

Social Networking Services have seen an unprecedented adoption rate in the world of information technologies. This adherence has been so strong that even new psychiatric pathologies have been risen around them. Notwithstanding the numerous benefits of using social networking services, these systems live from information share between their users, and very often this information is private. Although social network services have numerous privacy and security settings, and management features, many users choose - consciously or unintentionally - to make excessive or uncontrolled sharing of personal information with social network services. This supposed controlled sharing of personal information on social media can put people at risk, or even in threatening situations, either to the individual himself or to others, linked to his network or family. An exploratory study was conducted through a focus group involving 12 college students attending the first year of an undergraduate program. This study aims, particularly, to understand how college students perceive their own online exposition, and the importance that this has on their privacy and the security of information shared, in social networking services. The data gathered from the focus group was analyzed with an online content analysis software – using the Leximancer platform. From the content analysis of the focus group several important concepts emerged: social network companies, location information, information sharing and distribution, user awareness changes. Findings suggest students are getting a new approach to privacy concerns over social media. Even though they are aware of the risks inherent in over-sharing private data, when faced with "to share or not to share" very often they tend to overlook the privacy concerns in favour of the social exposition. The obtained items and concepts were also used to develop a questionnaire, to be answered by a population of college students, in a subsequent study.

Keywords: Social Networking Services, Social Media, Online privacy, Perceived Privacy, Trust in Social Networking Services, Information Control

1 INTRODUCTION

In 1993 through the hands of an American magazine cartoonist[1] a popular metaphor was born – On the Internet, nobody knows you're a dog – on this cartoon we find two dogs (one of them using a computer) discussing the advantages of Internet and anonymity, this cartoon became a popular symbol for the Internet privacy, something that was implicit in the use of the Internet at the beginning of mainstream Internet. Years later in 2015 we find on the same magazine a new cartoon, featuring a similar pair of dogs watching their owner at a computer, this time one of the dogs asks to the other "Remember when, on the Internet, nobody knew who you were?".

These two cartoons pretty much represent the evolution that occurred in the Internet landscape on the last 20 years towards online user's information. This evolution has been based in the continued erosion of privacy, fuelled by a medium where no government intervention is actually effective, leaving privacy at the hands of the free-market forces, enabling the scenario where the amount of privacy online will continue to decline over time and that privacy will be more and more expensive to maintain [1].

Although it has been increasingly easy for companies and organizations to collect online user's information on their own systems, the peak to user's personal data collection is social networking systems, namely, online social networks. "If you're not paying for it, you became the product" [2].

Since its beginning social networking services such as Facebook, Twitter, LinkedIn, Pinterest or Instagram, have attracted millions of users. For many people using social networks online, the use of these platforms became part of their daily routines. With the massification of mobile technologies, there

[1] Peter Steiner, cartoonist and contributor to *The New Yorker* since 1979.

has been a growing ubiquity of social networks in people's daily lives. This omnipresence is so intense that in some cases even truly obsessive pathologies can develop [3] [4].

Well since the beginning of the massification of the Internet (1995) it is known that intensive exposure to the world wide web causes the decline of family communication, the reduction of social circle and an increase in depression and loneliness of individuals [5]. It is precisely this contraction of the social circle that impels the use of social networks in order to compensate for the social deficit. Social networking sites are excellent means for the development of multiple weak links, in turn these weak ties are great vehicles for obtaining information and opportunities [5].

A social networking site is an Internet-based service that allows people to build public or semi-public profiles, create lists of other users with whom they share a connection, view and cross-check their connection lists with those of other users, all these iterations occur within a limited system [6]. Social networking sites are the pinnacle of the "privatization of sociability" [5], that is, they expedite the reconstruction of the social circle through an individual-centred community, as a kind of social geocentrism.

The creation of the first social networking site in 1997, "SixDegrees.com", showed a great desire of people for this type of technology, this led to the appearance of hundreds of social networking sites, which in some cases grew so quickly that they attracted the attention of both the media and academia [6] [7].

Although social networks offer a whole range of interaction opportunities among their users, they also attract the attention of non-users, particularly for issues related to privacy and security. These concerns can be effectively substantiated, however, social networking sites have long since ceased to be niche phenomena [8], millions of people around the world consciously and voluntarily use these social networks to communicate, find friends, make appointments and look for jobs. By doing all these activities, they deliberately reveal highly personal information not only to acquaintances but also to strangers - for example - birth dates, mobile phone numbers or the current address are common data in social networks [9] [10].

We cannot but marvel with the nature, quantity and detail of personal information that some users provide, at the same time we must consider how informed this information sharing is [8]. There is a low awareness of users on how to protect their personal information on social networks [11] and do not always have a clear idea about who has access to it or how it can be used [12].

More than 40% of social network users share private information [13], this information may be shared and used without the express consent of the owner, making users vulnerable to various online threats such as fraud, identity theft, phishing, among others. Once information is placed on a social network, it ceases to be effectively private [14].

Having already registered growth rates of 3% per week [15] and being the largest repository of photos on the Internet, Facebook is undoubtedly the *de facto* social network, this hegemony of Facebook also increases its attractiveness to criminals, having arisen several pieces of software capable of launching automated attacks that allow identity theft or profile cloning [15].

In addition to personal information, social networks also allow the sharing of content, knowledge and experiences. This personally identifiable information can also quickly feed the profile design or serve as critical mass for commercial or political purposes without the users' knowledge.

Having a private and secure profile seems like a good idea for more conscientious users, but their connections with others and affiliations with public groups can also pose a threat to their security, as it is possible to exploit social networks to predict personal and sensitive information based on public information [16]–[18].

Simultaneously with the unbeatable growth of social networking sites and growing security concerns arising from its use, we need to add to this mixture the mobile devices, which, with new technologies, create additional security and privacy problems when collecting and making available the users' private information in social networks, specifically the geographical location [10].

According to Shin [xx] the attitude of users towards social networks rests on three pillars:

- Security: User perception of security, defined by the extent to which a user believes that using a system will be risk-free.
- Privacy: Control of the flow of personal information, including the transfer and exchange of this information.

- Trust: Social network trust is defined as the user's willingness to be vulnerable to the actions of the social network system, based on the expectation that the social network system will perform a particular action important to the user, regardless of the user's ability to monitor the social networking system.

2 METHODOLOGY

The main goal for this research is to understand the perceptions on privacy, self-exposition and social network services on college students. This has been achieved through seven components: the perception of privacy; the perception of security; the trust relationship with the social network services; awareness (of privacy practices); data collection recognition; identification of unauthorized secondary use; the perception of risks.

We conducted an exploratory study using a focus group composed of 12 college students attending the first year of an undergraduate program. The gender distribution was 17% male and 83% female, the age interval was between 19 and 26 years. The students were informed that their participation in the study was voluntary and that no private or personal information was to be collected.

The choice of focus group as the instrument for this study showed to be the best approach for generating concepts, usually elusive in regular questionnaires [19]. The focus group was conducted through a semi-structured interview, below you can find some of the questions asked to the panel:

- Do you think the Internet poses privacy issues? What about social networks? What kind of problems?
- Is it safe to think that the information provided to social networking sites will not be changed by third parties?
- Are social media sites honest with users?
- Advertising a clear online privacy policy is important to make users aware? Why?
- Does the collection of personal information by social networking sites upset you?
- Do you think social networking sites market user data to other companies?
- Is it risky to provide private/personal information on social networking sites? Why?

The plan was to raise several themes and see how the different concepts were approached and related. Data gathered from the answers was then analyzed through Leximancer online platform, which is a text mining software used to extract meaningful concepts from non-structured textual content. Leximancer digests the text to find all possible concepts, then, we analyze and remove all concepts not significant for each question. We managed Leximancer to produce a graphic that links all the concepts.

3 RESULTS

3.1 Perceptions on privacy and self-exposition in social network services of college students

On the following graphic (see Figure 1) we can see a whole realm of concepts that emerged from our focus group. Through the exploration of these concepts we reach some results, next, we present the interpretation of the data obtained supported by extracts from the answers.

Users turn to social networks because they exist and know that this has a certain meaning for them as users, they know the kind of social networks that exist and know what is associated with them, they have that notion. This implies, if they know what it is, and have a sense of what social networks are, we already know why they go there, they go to: talk, publicize, participate in events, groups and chats, make comments, laugh, cry. In sum to disclose what they should and should not do [7], [20]–[23].

The concept “users” has an intersection with social networks, whereas the concept of companies does not, this might mean that users are “inside” social networks, they are closer to social networks, in extreme one could say they are the social networks, we thus see a merger between the social life and digital life of users [24], [25]. In short, users know what social networks are, but they get and stay onboard anyway.

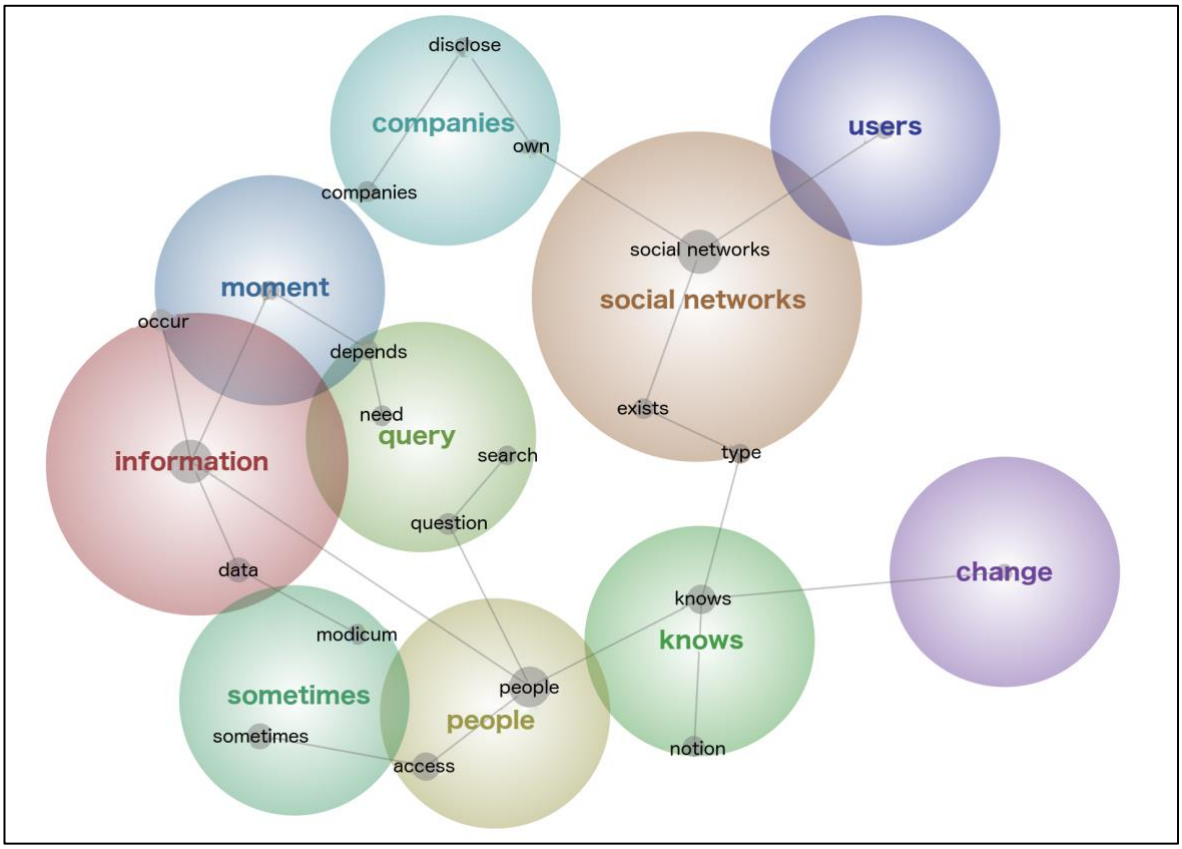

Figure 1. Analysis / Perception of privacy, self-exposition and social network services on college students

On the other hand, companies use social networks to publicize their own initiatives, always in their own interest. The concept “companies” does not interconnect with social networks, there is a gap, companies only use social networks, they are not part of it. Observe that users are also not connected to anything else other than social networks, so the concept of social networks is what connects users to companies. From the point of view of the companies this is excellent, they manage to capture the attention of users. From the point of view of users, it’s the usual story "I do not disclose anything, but everybody knows everything about me" [26] [27].

People know what social networks are and have a notion about it, funny that at the same time, there is here a notion of change, that is, we are facing a possible change in the notion (perception) of what is a social network, we are faced with a process of external change. Note that it is not in the users of social networks that this change is observed, it is in people. This shows a latent disassociation between the concepts user and person.

From the point of view of people, we see that sometimes they access social networks and in part they go there to seek information. People use social networks basically for queries, to look for information, but only sometimes, the rest of the time people produce information, this information can be text, images, videos, location information, etc...

On the one hand, people know that they can change and that they can somehow also cultivate their privacy, but on the other hand, they basically use social networks to exchange information. We are dealing here with a paradox [28], to what extent do people have the notion that by exchanging so much information they even know they can change. Do they really know they can change their privacy issues, their behavior and the way they react? In some way it is a kind of giving up, it’s almost like a feeling of apathy towards privacy [29] [30].

«… we are not going to change our habits even knowing that, therefore, this (privacy concerns) exist, we continue to live on the bubble and we accept that …»;

«… but there it is, if we think too much of course it concerns, but it is the question of conscious naivete, we do know the risks, but maybe we do not care so much …».

Another concept emerges, interacting on social networks is a matter of the moment, people can do something at a specific moment in time, yet for sharing something at that particularly moment the person might keep thinking about the consequences that it will have:

«… sometimes I do not share certain things (online) because I get that feeling in the subconscious and think that maybe they might be used against me, so I do not share so many things, but also it depends on the moment and place, there are times when we are doing things that we are so enthusiastic about what we are doing that we share without thinking …»;

«This is going to have other repercussions, for example we are now in college, but when we go to the job market, if the recruiting companies want they can do an investigation on us, and almost surely will find quite embarrassing things about us …».

There is this idea that what is lived at the present moment has already passed, and that in a way already belongs to the past, the problem is that it does not go away, it gets recorded in the social networks for future reference, and it will be recalled, eventually out of the initial context [25]. This moment depends on the need to look for questions, these questions can be affective or social, and as we see a bond between queries and information basically people are sharing and looking for everything that has to do with their personal life [22], [31].

On the graphic we do not find any privacy concepts, but it is quite relevant the focus attributed to the information concept (2nd largest dimension) it is because in fact students may even think that privacy is an important thing, but once they enter the social networks they forget about it.

Companies are between social networks and the moment, companies clearly take advantage of the moment, realizing the huge role of social networks helping them spread what they do, assume here a commercial role, taking advantage of the moments that people are living to exhibit what they do and at the same time get access to the information that users put on social networks.

It is curious that when the person puts himself in the role of the user his behavior changes, “one thing is what I do as a user, another thing is what people do”. People in general live the moments, look for various questions, share information, but they know what social networks are, notice that they know that at any time they can change. This dichotomy user *versus* person, is if the user and the person are two different things, this is to say, the privacy attitude and the privacy behavior are two different things [32]. This dichotomy is enhanced by the notion of the present moment, students tend to overestimate the present benefit of sharing information against the eventual future loss of privacy [21].

«… these people think that only what they put on the Net is going to appear, I think these people do not have this notion well …»;

«… I think there are people who think that just for example, Google has access to the data, they think it's just the phone that has the data and only there because it opened the application… »;

«… I have Facebook because there is no Messenger, and I have WhatsApp because it's the thing that my group at the University uses to communicate, as far as I’m concerned I would not use any of these social networks, I do not care, I don’t even publish anything …».

4 CONCLUSIONS

After the recent events of personal data breach that happened on Facebook, whose most popular is undoubtedly the Cambridge Analytica scandal [33], which exposed some serious implications that can happen over private/personal information gathered from social networks, this kind of work is increasingly urgent to spread and sensitize the community in general and academia in particular to the potential dangers of the invasion of social networks in the sphere of each citizen's own private life.

From our analysis to all the concepts about privacy and social networks that emerged from our focus group with college students, several conclusions can be made. First of all, what ties companies and users together are social networks, people know what a social network is and what type of social networks there are, there is even a change possibility in the horizon for new privacy behaviours to start happening. Meanwhile people are sharing and collecting information of their moments and their social network moments. These moments in time are faced as belonging to the distant past, almost as disappeared. Although there is an increasingly concern for the future usage of this information, that it might create difficulties and constraints on the next stage of college students when they start entering the job market.

Finally, our focus group evidenced the discrepancy that exists between the role of the user of social networks from the role of people as information providers and consumers, they both are perceived as distinct beings, it's a typical "us and them", although evidently all users are in fact people.

Following this work, a questionnaire will be developed, and these findings should be confirmed with a subsequent inferential study.

ACKNOWLEDGEMENTS

The authors would like to express their gratitude to Ana Filipa Rodrigues and Sara Bonifácio for their invaluable assistance making possible the focus group.

REFERENCES

[1] R. T. Rust, P. K. Kannan, and N. Peng, "The customer economics of internet privacy," *J. Acad. Mark. Sci.*, vol. 30, no. 4, pp. 455–464, 2002.

[2] S. Goodson, "If You're Not Paying For It, You Become The Product," *Forbes*, 2012.

[3] C. S. Andreassen, T. Torsheim, G. S. Brunborg, and S. Pallesen, "Development of a Facebook Addiction Scale," *Psychol. Rep.*, vol. 110, no. 2, pp. 501–517, 2012.

[4] S. Stieger, C. Burger, M. Bohn, and M. Voracek, "Who Commits Virtual Identity Suicide? Differences in Privacy Concerns, Internet Addiction, and Personality Between Facebook Users and Quitters," *Cyberpsychology, Behav. Soc. Netw.*, vol. 16, no. 9, pp. 629–634, 2013.

[5] M. Castells, *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press on Demand, 2002.

[6] D. M. Boyd and N. B. Ellison, "Social network sites: Definition, history, and scholarship," *J. Comput. Commun.*, vol. 13, no. 1, pp. 210–230, 2007.

[7] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006, vol. 4258 LNCS, pp. 36–58.

[8] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," *Priv. Electron. Soc. 2005*, p. 11, 2005.

[9] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Comput. Human Behav.*, vol. 25, no. 1, pp. 153–160, 2009.

[10] J. M. Kizza, *Computer network security and cyber ethics*. McFarland, 2001.

[11] J. Nagy and P. Pecho, "Social networks security," in *Proceedings - 2009 3rd International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009*, 2009, pp. 321–325.

[12] B. Krishnamurthy and C. E. Wills, "Characterizing privacy in online social networks," *Proc. First Work. Online Soc. Networks (WOSP '08)*, pp. 37–42, 2008.

[13] N. Hajli and X. Lin, "Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information," *J. Bus. Ethics*, vol. 133, no. 1, pp. 111–123, 2016.

[14] A. Sadeghian, M. Zamani, and B. Shanmugam, "Security Threats in Online Social Networks," *Int. Conf. Informatics Creat. Multimed.*, pp. 254–258, 2013.

[15] L. Bilge, T. Strufe, D. Balzarotti, E. Kirda, and S. Antipolis, "All Your Contacts Are Belong to Us : Automated Identity Theft Attacks on Social Networks," *Www 2009*, pp. 551–560, 2009.

[16] E. Zheleva and L. Getoor, "To Join or Not to Join : The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles," *Security*, vol. 7, no. 1, pp. 531–540, 2009.

[17] A. Mislove, B. Viswanath, K. Gummadi, and P. Druschel, "You are who you know: inferring user profiles in online social networks," *Third ACM Int. Conf. Web Search Data Min.*, pp. 251–260, 2010.

[18] M. Kosinski, D. Stillwell, and T. Graepel, "Private traits and attributes are predictable from digital

records of human behavior," *Proc. Natl. Acad. Sci.*, vol. 110, no. 15, pp. 5802–5805, 2013.

[19] J. Kitzinger, "The methodology of Focus Groups: the importance of interaction between research participants," *Sociol. Health Illn.*, vol. 16, no. 1, pp. 103–121, 1994.

[20] N. B. Ellison and D. M. Boyd, "Sociality through social network sites," *Oxford Handb. Internet Stud.*, pp. 151–172, 2013.

[21] C. Hallam and G. Zanella, "Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards," *Comput. Human Behav.*, 2017.

[22] D. Boyd, *It's Complicated: The Social Lives of Networked Teens*. Yale University Press, 2014.

[23] D. Boyd, "Facebook's privacy trainwreck: Exposure, invasion, and social convergence," *Convergence*, vol. 14, no. 1, pp. 13–20, 2008.

[24] N. B. Ellison, C. Steinfield, and C. Lampe, "The benefits of facebook 'friends:' Social capital and college students' use of online social network sites," *J. Comput. Commun.*, vol. 12, no. 4, pp. 1143–1168, 2007.

[25] D. Rosenblum, "What anyone can know: The privacy risks of social networking sites," *IEEE Secur. Priv.*, vol. 5, no. 3, pp. 40–49, 2007.

[26] P. A. Norberg, D. R. Horne, and D. A. Horne, "The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors," *J. Consum. Aff.*, vol. 41, no. 1, pp. 100–126, 2007.

[27] H. Krasnova, E. Kolesnikova, O. Guenther, and O. Günther, "'It Won't Happen To Me!': Self-Disclosure in Online Social Networks," *Amcis 2009 Proc.*, p. 343, 2009.

[28] S. B. Barnes, "A privacy paradox: Social networking in the United States," *First Monday*, vol. 11, no. 9, p. 5, 2006.

[29] D. Boyd and E. Hargittai, "Facebook privacy settings: Who cares?," *First Monday*, vol. 15, no. 8, 2010.

[30] E. Hargittai and A. Marwick, "'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy," *Int. J. Commun.*, vol. 10, no. 0, p. 21, 2016.

[31] M. Madden, A. Lenhart, and S. Cortesi, "Teens, social media, and privacy," *Pew Internet …*, p. 107, 2013.

[32] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers and Security*, vol. 64. pp. 122–134, 2017.

[33] P. Greenfield, "The Cambridge Analytica files: the story so far," *The Guardian*, 2018.