Location-based Games as Interfaces for Collecting User Data

Sampsa Rauti and Samuli Laato

University of Turku, Turku, Finland
sjprau@utu.fi

Abstract. Location-based games (LBGs) are becoming increasingly popular. These games use player's physical location as a game mechanic, and many of the games are played in real time. This study investigates the affordances that three popular LBGs, *Ingress*, *Pokémon GO* and *The Walking Dead: Our World*, provide for users to collect location data from other players. To this end, the game mechanics of the games and the end user privacy policies are analyzed and compared together. The results reveal several privacy concerns which are not currently adequately addressed in the privacy policies of the games. As LBGs are becoming increasingly complex, the risk of unwanted player data collection opportunities rises, combating which is predicted to be a major design challenge for LBG developers in the future.

Keywords: Location-Based Games, Privacy, Time-stamped location data, Data leakage

1 Introduction

A location-based game (LBG) is a game in which the gameplay revolves around and is affected by the player's physical location. Today, LBGs are usually played with mobile devices, and, location-based mobile games such as *Pokémon GO* and *Ingress* have reached high popularity. By making use of augmented reality and encouraging players to move, LGBs can provide several benefits for the players, such as inspiring to learn about their environment [22] and increasing physical exercise [2]. When the LBG also has social features prompting players to work together or to compete with each other, social relationships between players can be created and maintained [8, 28]. However, these kinds of pervasive games blending with the physical world and promoting mutual interaction between players, also have their drawbacks. One potential downside pertains to the player's privacy and consequently their security.

The sensitivity of timestamped location-data has been discussed in academia recently [3, 12, 15]. Time-stamped location data can reveal a lot about users' movement and actions. LBGs have been claimed to collect this information in exchange for allowing players to play their game [11], but there is also a risk that end users utilize the game as an interface to spy on other players. Yet, in

a recent study of *Pokémon GO* players, it was found that privacy concerns do not negatively correlate with intentions to keep playing the game [10]. There are at least three possible explanations for this: (1) The users are not aware or do not fully realize the extent of personal information they are giving away while playing [1], (2) Those concerned with their privacy do not begin to play in the first place and thus do not respond to such a questionnaire or (3) Users are aware they are giving away their privacy but do not care [1, 13]. The last option might be the most logical explanation, as the mobile phone has so many apps collecting sensitive information all the time that keeping track of them all is impossible, and thus it is easier to just resign the attempt to maintain any privacy [13]. It has also been suggested that instead of seeing the disclosure of location information as a privacy threat, it can actually give the player a feeling of controlling one's surrounding area and a sense of security [6].

The aim of this study is to investigate the affordances that currently popular LBGs provide for other users on collecting location-related sensitive data from players. To identify the affordances for players to spy on their peers, the game interfaces and all shared data is observed in three selected case games. The privacy policies of the games are also read with the purpose of identifying how they take privacy concerns related to the users location into account. The findings of this study are expected to bring transparency to the possibilities of leaking personal time-stamped location information to the public through LBGs and what potential harm this may bring to players.

The rest of the paper is organized as follows. Section 2 discusses the research design, defines important terms, introduces the case games of the study and presents the research methods. Section 3 discusses the results, describing the affordances the studied case games have for data collection by other players. An analysis of privacy policies of these games is also provided and the found affordances are compared with the statements made in the privacy policies. Section 4 discusses the possible ways the acquired location-based data can be used, implications for society and limitations of the study. Finally, Section 5 concludes the paper and suggest topics for future work.

2 Research Design

Previous studies on privacy in LBGs have focused mainly on how the developer of the games can collect sensitive information from the players (e.g. [11]). Figure 1 illustrates that this is only one side of the privacy concerns in LBGs. Thus, we supplement the previous studies by focusing on how third parties, or players themselves, can use these games as interfaces for sensitive data collection from other players. We sort these risks into two categories as shown in Fig 1: intended (controlled) and unintended. For the purpose of discovering data collection opportunities in LBGs for 3rd parties, we look at the game mechanics of three popular and unique LBGs *Pokémon GO*, *Ingress* and *The Walking Dead: Our World*.

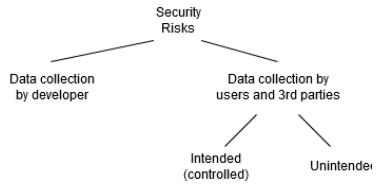

Fig. 1. A high-level categorization of the privacy risks in location-based games.

2.1 Definition of Terms

The definition of game mechanics by Sicart [24] being *methods invoked by agents for interacting with the game world* is adopted. All three games contain virtual points of interest (PoIs) which are located in geographical locations in the real world [17]. Travelling to these PoIs and moving around to find new ones can be regarded as the main gameplay.

Also a definition for the term affordance is required. The word affordance at its core describes the physical interaction between objects and people [21]. The inventor of the word, Gibson, originally limited the meaning of the world only to real, existing properties but later Norman expanded the meaning to also cover perceived properties [18]. In this study we limit the analysis to the domain of real empirically verifiable affordances as defined by Gibson [18] as we observe LBG game mechanics to identify real opportunities for collecting location data from players.

2.2 Case Games

Of the three case games, *Ingress* is the oldest being released for beta in 2012 and fully in 2013. The game focuses on navigating to PoIs called portals, capturing them and linking them together to form triangles. *Ingress* monetized itself by crowdsourcing the development of a global database of geographical virtual PoIs [16], which proved to be a good strategy as the same PoI database was later used in the smash hit *Pokémon GO* [17]. *Pokémon GO* was released in summer 2016 and is currently regarded as the most popular LBG of all time in terms of number of installs, total revenue created and the number of active players. In the game the user is tasked to move around to find pokémon spawns which can be captured and collected via completing a ball throwing minigame. Since its release the game has been updated heavily and many new features have been added. The final game, *The Walking Dead: Our World*, is different from the two previous games in the way that its PoIs are not based on real world objects [17]. However, gameplay-wise it is similar, as users move around to find PoIs and clicking them initiates a minigame which allows players to obtain rewards.

2.3 Methods

The game mechanics [24] of the case LBGs are analysed and used to define affordances for user-data collection, focusing specifically on how other players can harness the multiplayer elements of LBGs to collect sensitive location-related information from other players. Identified scenarios of how location-related data (both intended and unintended) from users can be retrieved and used by other players are presented.

Previous studies looking at privacy policies have almost explicitly found them to be difficult for users to understand [29]. However, in many cases users merely glance through the policy without reading it carefully [25]. Studies have found privacy policies to be sometimes intentionally vague and have developed frameworks for identifying these spots [23]. We study the privacy policies of the case games to identify and record all paragraphs where sharing location based data with other users is discussed. Loosely based on the approach of Shvartzshnaider et al. [23], these paragraphs are then analyzed to find vague points in the text where the privacy concerns are not addressed in sufficient detail. The affordances of game mechanics to collect user data and the information retrieved from the privacy policies are then compared.

3 Results

3.1 Affordances of LBG Game Mechanics for Data Collection by Other Players

Pokémon GO Since its initial release in 2016, *Pokémon GO* has been updated over a hundred times with several new game mechanics and content being introduced, making it a complex game. Thus, the opportunities the game provides for following its players' locations are many-fold. This section presents the game mechanics which were found to, at least in some way, reveal sensitive or private information about players' whereabouts to others.

In *Pokémon GO*, gyms are PoIs scattered throughout the map where trainers battle the pokémon of opposing teams for control over the gyms. Looking at the information in gyms is the most obvious way for the players to get other players' location information. In every gym, the players currently holding the gym and the time they visited the gym are displayed. This information can be used to track players' movements as seen in Fig. 2.

Lures are another mechanism that discloses the location of the player who deploys them. A lure module is attached to a pokéstop (a type of PoI) and it attracts pokémon for 30 minutes. During this time, other players can see the name of the player who has activated the lure module. The player can also usually be quite easily found in the real world location of the pokéstop, which makes it possible to connect the player's nickname to the real person.

Raids, in which trainers fight a powerful pokémon together, also offer a possibility to find out more about the real people behind nicknames. In the raid lobby, a player can see nicknames of other players preparing for the raid, as well as three

Fig. 2. The Gyms in Pokémon GO display the unique player name and deployment time, thus providing time-stamped location data where the player was at the given time.

statistics of the players: battles won, pokémon caught and distance walked. Because raids gather people together in the physical world, trainer nicknames can be connected with real persons in a manner similar to lure locations.

Befriending people in-game discloses even more information about a player. Gathering new friends is not only possible in real world but also online simply by exchanging player codes, which facilitates befriending strangers and potentially collecting information about them. Therefore, a malicious actor could distribute his or her player code with the aim of gathering sensitive data.

Pokémon GO includes gifts that can be exchanged between friends. When opening a gift, the location of the PoI from which the sender who picked up the gift is revealed. This way, friends can obtain information on the player's location and the routes they usually take. This can be done from the other side of the world, and an adversary can find out the exact locations frequently visited by the player by gathering pokéstop data from gifts, and then using a tool such as Ingress Intel Map [19], that displays the PoIs and their locations in a certain area, to find where exactly these pokéstops are located. It is also worth noting that as there is lots of contextual information (such as a PoI title, an image and a description) associated with each pokéstop player has visited, the adversary

can also derive additional information from this data. For example, the location of the player's home and workplace could be revealed.

Friends can see which pokémon the player has caught last, as well as battles won, distance walked and pokémon caught. All this information is updated in real time, so the friends can see when the player is playing the game. The recently captured pokémon and their types might give the adversary clues about the player's location. For example, if a player catches a pokémon that can only be obtained from a raid at certain time, the adversary can deduce where the raid has taken place in player's home area. There are also regional pokémon in the game, and seeing these in the recently caught pokémon list can reveal that the player is currently travelling. However, *Pokémon GO* currently allows players to disable the feature which shows friends their recently caught pokémon.

The Walking Dead: Our World In the *Walking Dead: Our World*, players currently have only a single method of revealing their location to everyone, that is, to place houses on the map or place survivors in them. Even so, there is no time-stamp to these actions, making it really difficult to collect data from other players whereabouts. The game does, however, contain social features which are currently limited to the players group. Joining a group is voluntary, and sharing information in the group is also voluntary. If the player so chooses, they can reveal their location to others via placing a *flare* or revealing their location in the chat. However, no other forms of revealing ones location currently exists in the game.

Ingress Prime *Ingress*, sometimes also referred to as *Ingress Prime*, differs from the other two games in that it openly broadcasts almost all player actions to every other player via a communication channel called COMM. These actions are time-stamped and the location of the actions is also provided, meaning players are able to follow each other effectively. As previously mentioned, in *Ingress*, players are tasked to travel to PoIs called portals, capture them and link them together to create fields. There are currently two teams in the game and destroying portals, links and fields from the enemy team is a major part of the game as well. Players can also deploy items called *frackers* on portals to double the amount of items they receive from *hacking*.

Players' actions can be visualised using official tools provided by Niantic such as the Ingress Intel Map [19] or unofficial community developed tools such as Ingress Intel Total Conversion [7]. The following player actions are visible to others directly through the communication channel of the game: (1) capturing a portal, (2) creating a link, (3) creating a field, (4) destroying a portal, (5) destroying a link, (6) destorying a field, (7) any messages sent in COMM (unless private) and (8) placing a *fracker* on a portal.

On top of these, players can indirectly follow each others movement by, for example, observing how their AP (Actions Points, measures players progress and is rewarded from almost all in-game actions) increases which reveals charging or hacking portals, or by looking at XM (Exotic Matter, disappears from the

ground when a player collects it) in the ground which reveals player's movement. Because players' actions are publicly visible to others, players might be more consciously aware of it and avoid playing a certain way or playing at all when they do not wish to reveal their location.

3.2 Analysis of privacy policies

Niantic's privacy policy [20] contains a paragraph describing the data shared with other players. The privacy policy states that *"when you use the Services, and in particular when you play our games, use social features within those games, or take part in live events, we will share certain Personal Data with other players."* The concept of personal data is further elaborated as follows: *"This Personal Data includes your in-game profile (such as your username, your avatar, and your team), your in-game actions and achievements, the real-world location of gameplay resources you interacted with when playing the games (for example PokéStops within Pokémon GO, Fortresses within Harry Potter: Wizards Unite, or Portals within Ingress), and your public in-game messages."*

The privacy policy also gives some additional game-specific information about the data shared to other players: *"When you take certain actions in Pokémon GO and capture a Gym, your (or your authorized Child's) username will be shared publicly through the game, including with other players, in connection with that Gym location."* This statement is vague, as the meaning of "certain actions" is left completely unexplained. It also leaves out many features currently implemented in the game such as lures, raids and all the information friends of the player can see.

In Ingress, the game discloses *"your in-game username, messages sent to other users in COMMS, and in-game portals that you interact with, as well as your device location whenever you take an in-game action."*

Niantic's privacy policy is vague at many points. While the text is detailed at times, such as when explaining the data shared to others in a gym, the description is mostly not that comprehensive, failing to define "in-game actions" and "achievements" specifically, for example. The significance of time (e.g. the fact that it is often possible to see when the players visited a specific PoI) and the contextual information (e.g. in the PoI descriptions) is also ignored in the text. Only after playing the games and learning their core mechanics can a player fully appreciate what the actions taken in the game mean in terms of privacy.

When it comes to data shared to other player's, Next Games's privacy policy [9] seems to be even more vague: *"Social features are a core component of our games. Other players and users may, for example, see your profile data, in-game activities, leaderboard position and read the messages you have posted."* The text does not refer to location or time at all, although it does mention that in-game activities are shared.

3.3 Comparison Between Affordances For Data Collection and What the Privacy Policy Says

In Table 1 we have sorted the findings of previous sections into three categories: (1) time-stamped location data, (2) contextual data and (3) circumstantial evidence. The time-stamped location data is the most accurate and can be used to identify with certainty, assuming the player is playing with their own account, where the player was at a given time. Contextual data and circumstantial evidence are less accurate, but when combined with other information, they can be used to derive information such as where the player lives or works or even the accurate location of the player.

Table 1. Categorisation of what types of location data the case LBGs yield to other players

Category	**Examples of Found affordances**
Time-stamped location data	Player actions in Comm (Ingress), Deployment times at gyms (Pokémon GO), Flares (The Walking Dead)
Contextual data	Gift locations and descriptions (Pokémon GO) Disappearing XM (Ingress)
Circumstantial evidence	Capturing regional Pokémon (Pokémon GO), Deploying buildings (The Walking Dead), Increasing AP, acquired medals (Ingress), player profiles (All games)

The main differences between the observed affordances for data collection and contents of privacy policies can be summarized in the following items:

- *Features.* It appears privacy policies either completely omit the explanation of privacy implications of specific features of the studied games by using general terms such as "in-game actions", or alternatively only mention few selected features (such as gyms in the case of *Pokémon GO*). While it is understandable privacy policies covering several games aim to be generic, some pivotal affordances for collection of private data, such as friends in *Pokémon GO*, should be better covered in privacy policies regarding their privacy implications.
- *Time.* The studied privacy policies do not mention the temporal dimension at all. Both real-time observations (e.g. alerts in *Ingress*) and time-stamped data on the past events (e.g. time of placing a pokémon in a gym) fall into this category. The fact that time-stamped location data could be extracted from the game could be explained better.
- *Contextual data.* Niantic's privacy policy mentions the contextual data sometimes delivered along with the player's location. However, the implications

of contextual data, such as the potential disclosure of player's daily routine and places they frequently visit is not discussed in any way. The contextual information associated with PoIs helps the adversary to gather useful information even when they are not familiar with the environment where the player plays the game.

– *Combining pieces of information.* While some LBGs such as Ingress readily broadcast alerts on the player actions in a certain area, some games such *Pokémon GO* require more work from the adversary to combine all pieces of the puzzle and to profile a player's movements and daily routine. Although it is not the purpose of privacy policies to instigate threat scenarios, more care should be taken to make players understand that the pieces of data in games can potentially be used against them. In complex systems, it may also be legally unclear who (companies or people) is responsible for potential abuse of acquired data.

4 Discussion

4.1 What can be done with the shared location data?

The easy accessibility of a player's location information to other players can be employed for malicious or commercial purposes. For example, an adversary might use a horde of bots (automatic programs posing as players) to track the movements of players. This might not be as accurate as the game developers database on player locations and in-game actions, but it is still an effective way to track active players.

Empirical evidence of this was obtained in 2017 when a whistleblower in Ingress revealed large scale use of a datascraping tool called *Riot*, which was used to spy on fellow player's movements and actions [5]. APIs for accessing game data have been developed for other games besides Ingress[1] too (e.g. Pokémon GO[2] [3]). At the end of 2019, Ingress Player Tracker database was widely advertized in Ingress communities. Purchasing access to the database allows tracking all players' movements and activity.

Thus, while Niantic, for example, only shares *"anonymous data with third parties for industry and market analysis"*, malicious parties might acquire unanonymized information without permission by using the game as an interface for data collection. Depending on the objectives of the adversary, this can be done to gather large amount of data on all players generally or to spy on specific players.

The acquired location data could be used to identify where players move on their daily basis, when they are travelling, with which other players do they play together and so on. Simply revealing player's home address or workplace location can be an issue, as demonstrated by, for example, *swatting*, that is, using

[1] https://github.com/IITC-CE/ingress-intel-total-conversion
[2] pogo api: https://github.com/Grover-c13/PokeGOAPI-Java
[3] https://github.com/rubenvereecken/pokemongo-api

a fake excuse to call the United States' *Special Weapons and Tactics Squad* on a person's home [14]. Besides illegal use of the data, it could be used to identify commercial opportunities and solve problems such as when and where to setup a food truck.

4.2 Implications for Society

Playing LBGs blends with everyday activities, thus increasing the value of personal location data acquired through the game. The ubiquitous presence of data collection in the digital society makes it impossible for individuals to be aware of where everywhere their personal data is being held, despite legislation such as the European Unions GDPR [26] offering users the possibility to retrieve their personal data from companies. Still, legislation such as GDPR can help mitigate the negative impacts of known intended data collection. The problem with unintended data collection opportunities remains, and, therefore, companies providing open interfaces containing sensitive information such as location data should be careful about the affordances of such an interface for malicious purposes.

More and more services are being focused to the mobile phone. Identification and banking services, communication and games are just few examples of what an increasingly large quantity of users are using their phones for. Gaining access to a modern person's mobile phone essentially means getting hold of their entire life. Therefore, constantly donating personal location information for the world to see via playing LBGs can expose players as easy targets to burglars or even muggers [4]. While it is generally a positive thing to increase the quality of virtual PoIs in pervasive technologies such as LBGs [22, 17], this can also increase the opportunities for identifying user movement patterns and propensity. A real life example is the removal of a pokémon gym from Pentagon, as defense officials were concerned that playing *Pokémon GO* inside the building could give away sensitive information such as room locations [27].

4.3 Limitations

This study is limited by its scope of looking only at location-related sensitive data, instead of sensitive data more holistically. Also only three popular LBGs were looked at, and accordingly, our findings are tied to these games despite attempts to generalize the findings. We observed the current state of the games and privacy policies, however, both are subject to change and thus the results of this study depict the current state of affairs. Due to the technical complexity of the games, and the architecture of the games not being publicly available, room for speculation remains as to whether there are technical exploits or other unintended ways to obtain sensitive information from players which were not covered in this study.

5 Conclusions and Future Work

With our findings we confirmed the following:

- Location-based multiplayer games can be used as interfaces to gather detailed information on location and movements of players.
- Privacy policies provided by game development companies are often vague and lack details and information on the possibilities of other players or third parties to obtain the player's private information.

LBGs have been around for over 10 years, but information collection through them is still a relatively fresh topic. Minor cases of location-data abuse have been reported, however, currently there is no evidence that data from LBGs would have been systematically used for malicious purposes. Currently LBG players are not concerned with leaking sensitive information such as time-stamped location data online while playing [10]. This could change in the forthcoming years unless negative aspects of users location-data leakage can be mitigated. The findings of this study urge LBG developers to ensure their games cannot be used as interfaces for player location surveillance.

References

1. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science **347**(6221) (2015) 509–514
2. Althoff, T., White, R.W., Horvitz, E.: Influence of pokémon go on physical activity: study and implications. Journal of medical Internet research **18**(12) (2016) e315
3. Brown, J.W., Ohrimenko, O., Tamassia, R.: Haze: Privacy-preserving real-time traffic statistics. In: Proceedings of the 21st ACM SIGSPATIAL international conference on advances in geographic information systems, ACM (2013) 540–543
4. D'Anastasio, C.: Pokémon go streamer mugged live on twitch [update] (2016)
5. D'Anastasio, C.: Ingress players use unofficial tools to stalk one another (2017)
6. De Souza e Silva, A., Frith, J.: Location-based mobile games: Interfaces to urban spaces. Frissen, Valerie/Lammes, Sybille/De Lange, Michiel/De Mul, Jos/Raessens, Joost (Hg.): Playful Identities. Ludifizierung von Kultur (2015)
7. developed, C.: Ingress intel total conversion. [ONLINE], available at https://iitc.me/, checked 6th of November, 2019 (2019)
8. Finco, M.D.: I play, you play and we play together: Social interaction through the use of pokémon go. In: Augmented Reality Games I. Springer (2019) 117–128
9. Games, N.: Privacy policy. [ONLINE], available at https://www.nextgames.com/privacy-policy/, checked 11th of November, 2019 (2019)
10. Hamari, J., Malik, A., Koski, J., Johri, A.: Uses and gratifications of pokémon go: Why do people play mobile location-based augmented reality games? International Journal of Human–Computer Interaction **35**(9) (2019) 804–819
11. Hulsey, N., Reeves, J.: The gift that keeps on giving: Google, ingress, and the gift of surveillance. Surveillance & Society **12**(3) (2014) 389–400
12. Jedrzejczyk, L., Price, B.A., Bandara, A.K., Nuseibeh, B., Hall, W., Keynes, M.: I know what you did last summer: risks of location data leakage in mobile and social computing. Department of Computing Faculty of Mathematics, Computing and Technology The Open University (2009) 1744–1986

13. Kang, R., Dabbish, L., Fruchter, N., Kiesler, S.: "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In: Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015). (2015) 39–52
14. Karhulahti, V.M.: Prank, troll, gross and gore: Performance issues in esport live-streaming. In: DiGRA/FDG. (2016)
15. Kulik, L.: Privacy for real-time location-based services. SIGSPATIAL Special **1**(2) (2009) 9–14
16. Laato, S., Hyrynsalmi, S.M., Paloheimo, M.: Online multiplayer games for crowd-sourcing the development of digital assets - the case of ingress. In: Software Business - 10th International Conference, ICSOB 2019, Jyväskylä, Finland, November 18-20, 2019, Proceedings. (2019) 387–401
17. Laato, S., Pietarinen, T., Rauti, S., Laine, T.H.: Analysis of the quality of points of interest in the most popular location-based games. In: Proceedings of the 20th International Conference on Computer Systems and Technologies, ACM (2019) 153–160
18. Lee, J., Bang, J., Suh, H.: Identifying affordance features in virtual reality: How do virtual reality games reinforce user experience? In: International Conference on Augmented Cognition, Springer (2018) 383–394
19. Niantic: Ingress intel map. [ONLINE], available at https://intel.ingress.com/intel, checked 6th of November, 2019 (2019)
20. Niantic: Niantic privacy policy. [ONLINE], available at https://nianticlabs.com/privacy/, checked 11th of November, 2019 (2019)
21. Norman, D.A.: Affordance, conventions, and design. interactions **6**(3) (1999) 38–43
22. Oleksy, T., Wnuk, A.: Catch them all and increase your place attachment! the role of location-based augmented reality games in changing people-place relations. Computers in Human Behavior **76** (2017) 3–8
23. Shvartzshnaider, Y., Apthorpe, N., Feamster, N., Nissenbaum, H.: Going against the (appropriate) flow: A contextual integrity approach to privacy policy analysis. In: Proceedings of the AAAI Conference on Human Computation and Crowdsourcing. Volume 7. (2019) 162–170
24. Sicart, M.: Defining game mechanics. Game Studies **8**(2) (2008) n
25. Steinfeld, N.: "i agree to the terms and conditions":(how) do users read privacy policies online? an eye-tracking experiment. Computers in human behavior **55** (2016) 992–1000
26. Tankard, C.: What the gdpr means for businesses. Network Security **2016**(6) (2016) 5–8
27. Thielman, S.: Pentagon's pokémon orders: game must go (outside) for security reasons. [ONLINE], https://www.theguardian.com/technology/2016/aug/12/pentagon-pokemon-go-restrictions-security-concerns, checked 11th of November, 2019 (2016)
28. Vella, K., Johnson, D., Cheng, V.W.S., Davenport, T., Mitchell, J., Klarkowski, M., Phillips, C.: A sense of belonging: Pokemon go and social connectedness. Games and Culture **14**(6) (2019) 583–603
29. Winkler, S., Zeadally, S.: Privacy policy analysis of popular web platforms. IEEE Technology and Society Magazine **35**(2) (2016) 75–85