An Analysis of Facebook's Graph Search

Zubeida Casmod Khan
Department of Computer Science,
University of Cape Town, South Africa and
Council for Scientific and Industrial Research, Pretoria,
South Africa
zkhan@csir.co.za

Thulani Mashiane
School of Mathematics, Statistics, and Computer Science,
University of KwaZulu-Natal, South Africa and
Council for Scientific and Industrial Research, Pretoria,
South Africa
tmashiane@csir.co.za

***Abstract*—With over a billion active users monthly Facebook is one of the biggest social media sites in the world. Facebook encourages friends and people with similar interests to share information such as messages, pictures, videos, website links, and other digital media. With the large number of users active on Facebook, an upgrade to Facebook's searching capability was made through the launch of graph search. Graph search is a powerful search feature which allows users to search Facebook using queries phrased in simple English. When a query is executed, the results from the search can reveal personal information of friends as well as strangers. This availability of personal information to strangers is a cyber security threat to citizens. Cyber criminals can use the graph search feature for malicious and illegal intent. This paper presents an analysis of graph search on Facebook. The purpose of the study is to highlight the amount and type of personal information that is accessible through Facebook's graph search. This is done through the design and execution of graph queries on two separate Facebook profiles. An analysis of the results is presented, together with possible negative consequences, and guidance as to best practices to follow in order to minimise the cyber security threats imposed by Facebook's graph search.**

Keywords-Facebook, graph search, cyber security, cyber-criminal, stalking, spam, identity theft, authentication, cyber warfare.

I. INTRODUCTION

Facebook is a popular social media network that has become an integral part of our daily lives. People use Facebook to express themselves, connect with others, share content, pursue academic endeavours, and for marketing purposes. The term Social Search has been defined as the use of social mechanisms to find information online [1]. Social search engines involve searching for individuals who satisfy specified criteria.

Since its original release in 2004, the social search functionality of Facebook has come a long way. Originally, a user was restricted to searching for a person via their name, surname or email address. In March 2013, Facebook rolled out a new type of graph search, based on semantics, greatly improving search results by allowing users to find social activities of friends. Given the growth of Facebook usage, it is not surprising that efforts have been made to improve search functionality. Nowadays one can search for questions expressed in natural language. For instance, one is able to search for the following queries: *people who like ice-cream*, *friends who like skydiving and live in Johannesburg* etc. This advancement in search functionality, however, opens up a plethora of privacy and security concerns. Previous studies [4], [6], [7] describe privacy and security issues within Facebook. These issues also exist in Facebook's new graph search.

Facebook's graph search could also be used for cyber warfare purposes. Terrorists and hacktivists could use it to identify a targeted group of people with specialised criteria, such as location information, specific interests, age, and political views. This could be done in order to recruit potential members for an organisation, or to plan attacks targeting a particular group. Conversely, government and law enforcement agencies could use the graph search to assist with crime and terrorism investigations by designing specialised queries to locate criminals.

In this paper, we examine Facebook's graph search to determine the ease with which personal information can be acquired under different circumstances, by comparing the graph search results acquired from a Facebook account with no friends, to results of a mature account with an average number of friends. We analyse all the results to determine the negative effects of the search. The purpose of conducting such an analysis is to firstly assess how easy it is to acquire data from strangers on Facebook using Facebook's graph search. Secondly, we determine whether having an increase in Facebook friends results in an increase of such data (from strangers).

In the remainder of the paper, we first provide a background of Facebook's search infrastructure as well as privacy and security flaws in Section 2. Thereafter, in Section 3, we present an analysis of the graph search. In Section 4, we provide best practices for protecting personal information from Facebook's graph search and finally we conclude in Section 5.

II. BACKGROUND

Information about Facebook's social search is presented in official Facebook notes[1] [2]. Upon release in 2008, the search

[1] https://www.facebook.com/notes/facebook-engineering/under-the-hood-building-out-the-infrastructure-for-graph-search/10151347573598920

[2] https://www.facebook.com/notes/facebook-engineering/

facility on Facebook was called PPS. PPS was simply a keyword based searcher. In 2009, the PPS searcher was enhanced by a new product called Typeahead. Typeahead predicted search queries based on the prefix that the user had typed in. In March 2013, graph search was released.

The data in Facebook's graph search is structured in a graph with nodes and edges. Nouns are represented by nodes, while verbs are represented by edges. For instance, a user *John Doe* may be represented by a node, the activity *lives in* may be represented by an edge, and the place *Pretoria* may be represented by another node. Different nodes may be connected to each other in different ways. Since the information in Facebook is linked in such a graphical structure, simple keyword usage is insufficient to conduct queries with keyword search due to a lack of semantic information. There would be great confusion when using keywords *John Doe Pretoria*. Could this mean, people named *John Doe* whose hometown is *Pretoria*, people named *John Doe* who lives in *Pretoria*, or people named *John Doe* who has studied in *Pretoria*? The way in which Facebook allows users to conduct queries with the necessary parameters is in natural language e.g., a query could be formulated as, *people named "John" who live in Pretoria*. Facebook processes the queries in three steps: 1. Entity recognition and resolution, 2. Lexical analysis, and 3. Semantic parsing. This is displayed in Fig. 1, for the query, *my friends, who live in San Francisco, California*.

Previously, cyber criminals had to execute technically extensive hacking methods in order to gain access to users' personal information. Today, however, accessing user information has been made easier through social networking sites with weak security implementations. Facebook has been criticised by researchers for having security vulnerabilities [4], [6], [7].

Studies on cyber warfare demonstrate that terrorists and hacktivists are actively using Facebook and other social media to plan attacks, recruit potential members, and contribute to cyber wars[2],[5].

A study on Facebook privacy among users of different ages [3] revealed that irrespective of age differences, users have open Facebook profiles without even realising it. It was found that users do not differentiate between sharing content between close friends and acquaintances.

In 2009, researchers had identified seven security threat dimensions in Facebook: Privacy and Confidentiality, Authentication and Identity Theft, Intellectual Property Theft, Vandalism, Harassment and Stalking, Defamation and Disparagement, Spam and Cybersquatting, Payment Transaction Integrity, and Malwares and Computer Virus [5]. These security vulnerabilities are also present in the graph search infrastructure of Facebook.

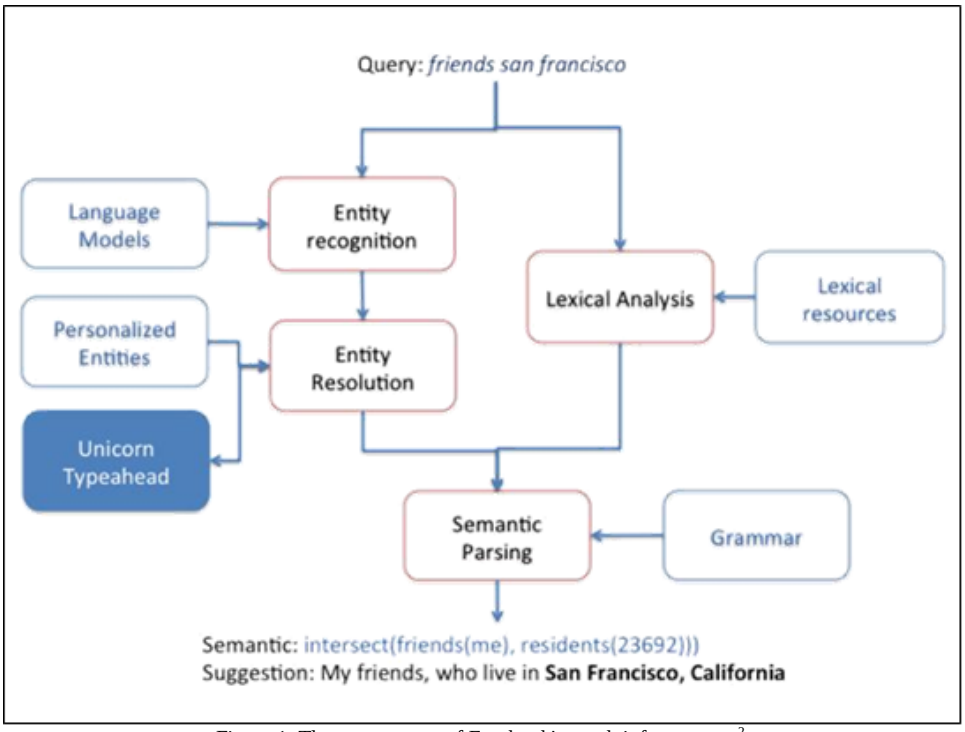

Figure 1. The components of Facebook's graph infrastructure[2].

under-the-hood-the-natural-language-interface-of-graph-search/10151432733048920

The security threat dimensions that are directly violated by the graph search feature in Facebook are Privacy and Confidentiality, Authentication and Identity Theft, Vandalism, Harassment and Stalking as well as Spam, which will be introduced in this section and discussed further in Section IV.

A. *Privacy and Confidentiality*

Privacy refers to the right of the users to select and control what and how their personal information is disclosed to other people. Confidentiality is making sure that users' personal information is kept secret, and is not shared with anybody else [12]. In 2012, Stutzman et. al [14] were able to collect profile data, over the period of five years, of users belonging to a particular group on Facebook. This was done through predictable network IDs that Facebook assigned to users when joining the network. For instance, if Facebook assigned a group ID of 42000 to a group each member that joined received an increment of that ID i.e., the first user would be 42001 and so on. This is an example of privacy and confidentiality breach because Facebook failed to keep their profile information from being accessed by other parties.

B. *Authentication and Identity Theft*

Authentication is being able to verify that a user profile belongs to a certain user [13]. Facebook has a login page for authentication. Identity theft is stealing the identity of another user. On Facebook this can be done by obtaining the username and password of the target profile and using them to login to Facebook, or cloning the target profile's account, by means of downloading their pictures and creating an identical profile. The newly created profile is then used to invite the target profile's friends and take advantage of the trust relationship between the target and their friends.

C. *Vandalism, Harassment and Stalking*

Cyber Vandalism is accessing a target page and making unauthorised changes to the page [13], [14]. On Facebook, vandalism is one of the consequences that arise when cyber-criminals gain unauthorised access to a targets profile. Harassment and stalking occur on Facebook when a cyber-criminal accesses a target profile's personal information such as username, email, telephone number or address to persistently and illegally contact the target.

D. *Spam*

Spam is sending unwanted bulk advertisement to a large number of users over the Internet [8]. On Facebook cyber criminals collect personal information such as email addresses from account profiles, and these accounts are then sent spam messages that could also contain malicious links.

E. *Social Engineering (Information Gathering Phase)*

Social engineering is defined as: "The science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where the social interaction, the persuasion or the request involves a computer-related entity" [10]. A social engineering attack is then defined as an attack employing either direct or indirect communication, and has a social engineer, a target, a medium, a goal, and one or more techniques [10]. A social engineering attack has six phases namely attack, information gathering, preparation, develop relationship, exploit relationship and debrief [11]. Facebook's graph search can be used in the information gathering phase where queries are executed specifically to find vulnerable people or to gather information about an identified person.

Facebook's privacy policy[3] states that they make certain categories of information publicly available and thus cannot be protected with privacy settings. This includes the pages that a user is a fan of, gender, current profile photo, album of cover photos, and networks that the user belongs to. This is vulnerability because such information is potentially dangerous in the hands of cyber criminals. These privacy and security concerns are magnified when taking into consideration Facebook's graph search which enables Facebook users to easily acquire and filter search queries, using categories such as demography, interests and so forth.

III. ANALYSIS OF FACEBOOK'S GRAPH SEARCH

We had hoped to make use of Facebook's existing developer tools such as Graph API, and Facebook Query Language (FQL). The former is the primary way to acquire data from Facebook and the latter is a SQL-styled tool to query Facebook's data. However, it was found that both the Graph API and FQL have limited search capabilities. A developer is not able to use these tools to pose queries in advanced natural language strings. The next step was to design and implement our own web crawler to search through public data. The first consideration to take into account was whether this was legal. However, it was found in official Facebook documentation[4] that automatic data collection in Facebook is prohibited unless one has written consent. Since automatically collecting data is prohibited, we restricted ourselves to designing a few search queries, and manually collecting and analysing results.

A. *Methodology*

The methodology for the analysis is as follows:

1) Create a new Facebook account, account 1, with zero friends. Do not add any data to the account besides what is necessary to sign up (First name, last name, email, birthday and gender).

2) Account 2 is an existing mature account with 272 friends.

3) Design search queries.

4) Conduct search queries for Accounts 1 and 2.

5) Calculate the number of results acquired for each query of each account.

6) Evaluate the results by:

a) Comparing the number of acquired results for each account.

b) Assessing the negative effects of each query security against the threat dimensions introduced in Section II.

[3] http://www.facebook.com/note.php?note_id=+322194465300

[4] https://www.facebook.com/robots.txt

TABLE I. CATEGORISING EACH GRAPH QUERY.

	Query	Basic Info	Living	Work and education	Likes and interests	Photos and videos	Relation-ships and family
1.	People who work at CSIR and live in Pretoria, South Africa		✓	✓			✓
2.	People under 18 years old who like Drinking and who live in South Africa	✓	✓		✓		
3.	Manga readers who live in Durban, KwaZulu-Natal		✓		✓		
4.	Single female Muslims who live in Johannesburg, Gauteng	✓	✓				
5.	People who were born from 1990 to 1991 and work at Sasol and live in South Africa	✓	✓	✓			
6.	People who live in Cape Town, Western Cape and like The Mortal Instruments		✓		✓		
7.	People who work as Tutors at UKZN and live in South Africa		✓				✓
8.	Women who were born after 1993 and live in Laudium, Gauteng	✓	✓				
9.	Females who were born after 1995 and visited Musgrave Centre and live in South Africa	✓	✓				
10.	People who interacted with photos of Economic Freedom Fighters and live in South Africa		✓		✓	✓	
11.	Females under 18 years old who checked in at Cafe Vacca Matta, Suncoast Casino and live in Durban, KwaZulu-Natal	✓	✓				
12.	Photos of men who work at CSIR and live in Gauteng, South Africa from April 2014	✓	✓	✓			✓

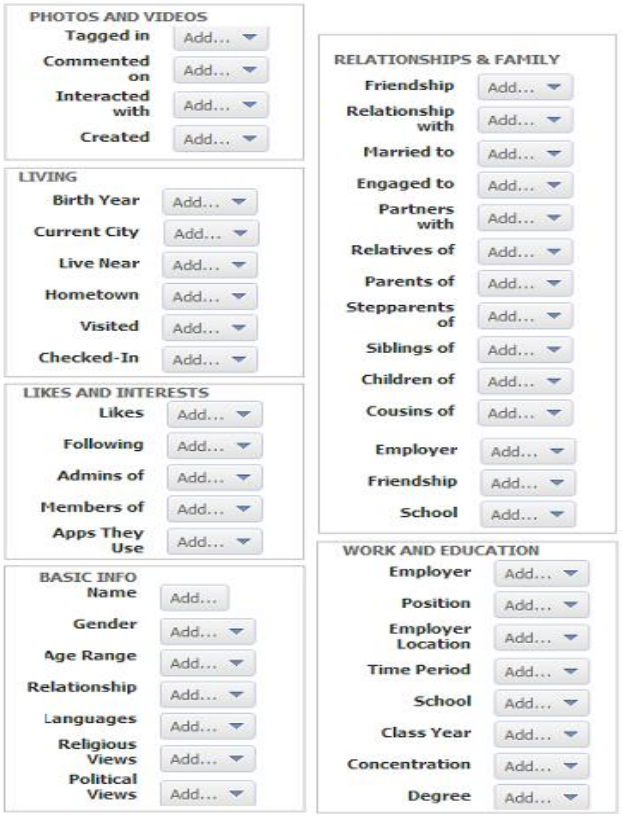

Figure 2. Criteria of Facebook's graphed data.

B. *Designing graph queries*

We wanted to design simple queries that would enable one to acquire a large volume of data with minimal effort. We formulated search queries based on using criteria from each category of Facebook's graphed data, displayed in Figure 2.

Each graph query together with its categorisation is displayed in Table 1. The queries are not formulated using proper grammar because they have to be in a simple form in order for Facebook to recognise the entities within the query. For each graph query, we restrict our results to locations in South Africa in order to acquire a manageable amount of data since the data collection and analysis are manual.

C. *Results and discussion*

For each query, the mature Facebook account, account 2, returns more results. This is because it includes results that are not publicly accessible and are returned due to friend relations and friend-of-friend relations. In most cases, few or no friends are included in the results for the queries in questions, yet many friend-of-friends are returned causing a large number of query results. In other words, one need not be friends with a user to obtain their information. The results returned for each query contain a user's name, a link to the user's Facebook account and some basic information.

TABLE II. A COMPARISON OF THE NUMBER OF RESULTS OBTAINED FOR EACH ACCOUNT.

	Query	Results from account 1	Results from account 2	Friends from account 2
1.	People who work at CSIR and live in Pretoria, South Africa	15	151	3
2.	People under 18 years old who like Drinking and who live in South Africa	0	4	0
3.	Manga readers who live in Durban, KwaZulu-Natal	248	303	2
4.	Single female Muslims who live in Johannesburg, Gauteng	21	60	0
5.	People who were born from 1990 to 1991 and work at Sasol and live in South Africa	18	>1000	1
6.	People who live in Cape Town, Western Cape and like The Mortal Instruments	121	143	1
7.	People who work as Tutors at UKZN and live in South Africa	8	39	0
8.	Women who were born after 1993 and live in Laudium, Gauteng	3	8	0
9.	Females who were born after 1995 and visited Musgrave Centre and live in South Africa	0	6	0
10.	People who interacted with photos of Economic Freedom Fighters and live in South Africa	n/a	n/a	n/a
11.	Females under 18 years old who checked in at Cafe Vacca Matta, Suncoast Casino and live in Durban, KwaZulu-Natal	0	2	0
12.	Photos of men who work at CSIR and live in Gauteng, South Africa from April 2014	0 (photos)	119 (photos)	3 (photos)

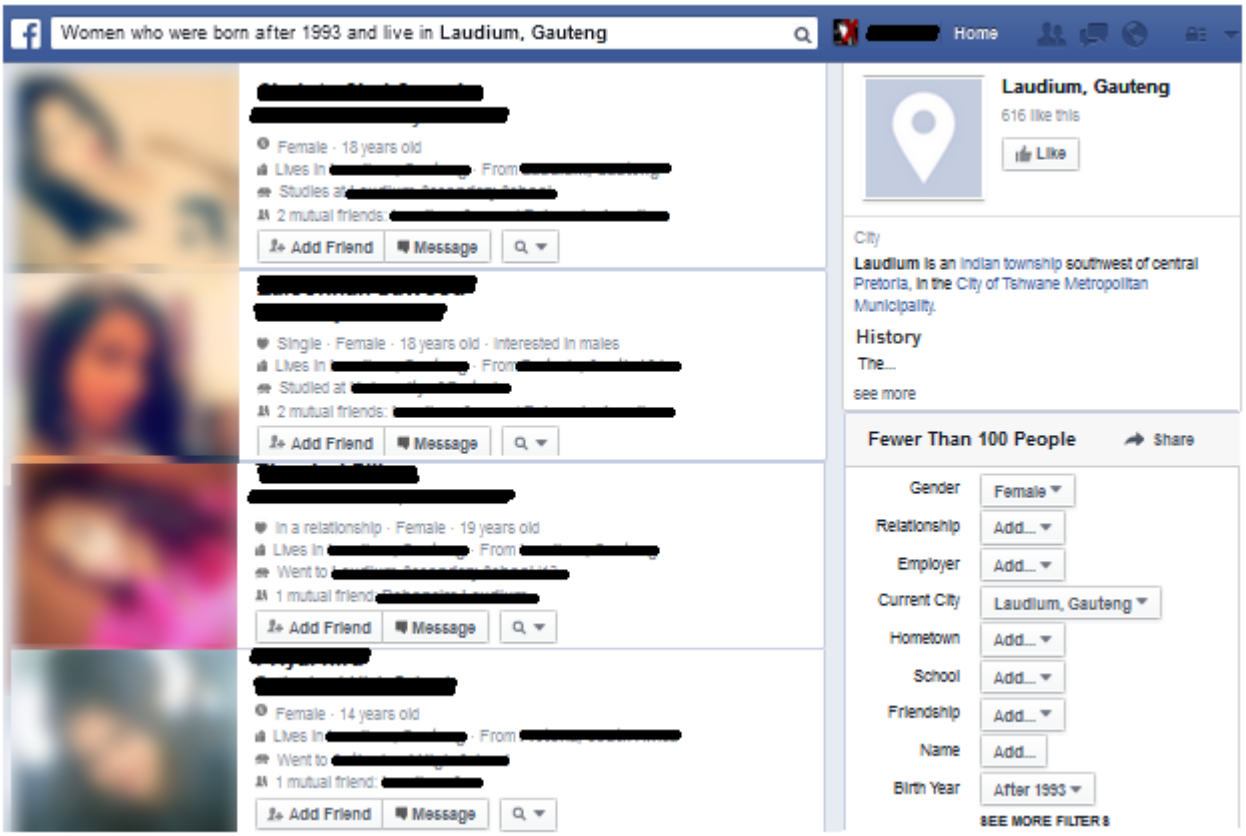

Figure 3. Partial graph search results for query 8: Women who were born after 1993 and live in Laudium, Gauteng.

This is displayed in Figure 3. Clicking on a user's account link opens up their profile and shows the user's data that is available. Even though account 1 returns significantly less results than account 2, there is still sufficient information that is publicly accessible. Account 1 did not return results for queries 2, 9, 10, 11 and 12. Account 2 returned results for all queries except query 10. Both accounts did not yield results for query 10 as the search query was not yet available by Facebook. Table 2 displays the comparison of the results for each account.

In Table 2, the first two columns represent the number of results obtained for each Facebook account. The third column, however, represents the number of friends from the results of account 2. We note that there are very few friend results from account 2 even though account 2 yields a high number of results. This means that most of the results from account 2 are strangers and friend-of-friends.

IV. THE NEGATIVE EFFECTS ON CYBER SECURITY OF EACH QUERY

In Section II a description of security threat dimensions of the graph search infrastructure of Facebook were presented. In this section, an analysis is done on how the queries in Section II fall into each of the security threats.

A. Privacy and Confidentiality

All of the queries can lead to privacy and confidentiality breaches. A user posts information on Facebook on the premise that it will only be viewed by other users who share a friend relationship. However, Facebook's graph search makes it possible for strangers to also view another user's private information without their knowledge. The retrieved profiles are public or accessible by friend-of-friends. Because of this, the information on the profiles is not confidential. This can have consequences on a person's professional life. For instance, interested parties can use query 11, *Females under 18 years old who checked in at Cafe Vacca Matta, Suncoast Casino and live in Durban, KwaZulu-Natal*, to screen students who are applying for scholarships and other prestigious opportunities. This kind of query could also tarnish relationships within families and friends.

B. Authentication and Identity Theft

Queries 1, 2, 4, and 5-12 all can cause Identity Theft. This type of information is exactly the type of information that can be easily retrieved using Facebook's graph search. The personal information revealed by these queries could be used to build a profile about the target user. This profile can be very accurate because the cybercriminal has the picture of the target user from their profile picture on Facebook, the region where they live as well as some of the target user's interests. This information can be easily used to create a clone Facebook profile.

C. Vandalism, Harassment and Stalking

All of the queries can lead to vandalism and stalking. Stalking is closely related to identity theft, where a cyber-criminal collects as much information about the target profile in order to act in a malicious or illegal way. For instance, if a paedophile wants to target children at a nearby location, the paedophile can simply use a query similar to query 8, *Women who were born after 1993 and live in Laudium, Gauteng,* and change the birth year parameters to a later year to target children specifically, which will return a list of children together with pictures that can be used as identification. It is extremely easy to link common whereabouts to people. The yoghurt bar, *Wakaberry*, coupled with the users' locations provides stalkers with the tools they need to locate targets. Stalkers could use query 4, *Single female Muslims who live in Johannesburg, Gauteng,* to look for people in a nearby area, who follow a particular religion.

D. Spam

All of the queries can lead to spam messages being sent to profiles. A cyber-criminal who is interested in spreading a virus into a company's network can use the results from query 5 to obtain a list of target employees. Using this list, the cyber criminal could send out spam messages with a malicious link in hope that one of the users in the list will click on the link.

Companies and spammers who are looking for a target group in a specific area can easily find candidates and message or befriend them through queries 1, 3, 4, 7, 10 and 11 as these queries connect a user's location as well as interests. Companies could use these queries for powerful target marketing and advertising.

E. Social Engineering (Information gathering phase)

All the queries can aid a social engineer to perform a social engineering attack. For example, if a social engineer was looking to attack an organisation, query 1 could be used to find vulnerable employees of that organisation, which could then be targeted and used as a channel to get to the organisation.

In this section we have discussed the implications of Facebook's graph search its users. It can be seen that the graph search feature can make a user more vulnerable to attacks by cyber-criminals.

V. BEST PRACTICES FOR FACEBOOK USERS CONCERNING GRAPH SEARCH

With the movement of web technologies to include semantics, one thing is for certain, Facebook's graph search is here to stay. Furthermore, as time progresses, users will be able to search for more advanced and specific queries. It is vital to protect data and information from the public. By default, Facebook sets general privacy settings to the weakest type available. Posts are set to public, and data can be seen by everybody. Therefore it is in the interest of a user to behave with caution, and monitor the settings of a Facebook account.

A. Restrict

First and foremost, though it may seem basic, a user should not accept friend requests from strangers. Even in the case where there are many mutual friends between the user and the inviter, one should not share day-to-day activities with a stranger. Secondly, on Facebook there are users that represent businesses and organisations. These Facebook users are in violation of Facebook's policies and should not be trusted. Companies and organisations are supposed to exist in the form of pages on Facebook. By accepting a friend request from a company in the form of a Facebook friend, the user allows the company total access to his profile data, whereas with a page, the user does not disclose profile data but only receives some updates from the page.

Facebook's check-in service allows one to share one's current location to friends, friend-of-friends or the public by checking in at popular places such as restaurants and malls. Users should not use Facebook's check-in service because it is a platform for cyber stalking. This is demonstrated for query 11, *females under 18 years old who checked in at Cafe Vacca Matta, Suncoast Casino and live in Durban, KwaZulu-Natal*. Using this query and its results, we prove that a stranger can find people based on check-in criteria for *Cafe Vacca Matta, Suncoast Casino*. If one has existing check-in and location information on a Facebook profile, it is best to remove this.

B. Limit

In the privacy settings category, most categories can be limited to the friend option. Using the friend-of-friend option is not safe, as demonstrated in the analysis in Section III, because it allows strangers to access one's data easily using the graph search. If aspects of a user's profile are not limited to friends only, strangers can easily access a user's profile using the graph search. For instance, one can search for a user based on a user's activity of liking *The Mortal instruments* (a book) when the user does not limit the like activity to friends only, as seen in query 6, *people who live in Cape Town, Western Cape and like The Mortal Instruments.*

C. Monitor

Facebook's graph search is still a work in progress. As time progresses, the type of queries a user is able to formulate will increase. It is up to the user to continuously monitor his privacy settings in an account and Facebook's privacy policy to detect potential threats. It is in the interest of the user to remain informed with Facebook's constantly changing privacy settings and new features to ensure that one's data is protected. For instance, consider query 10 in Section III; *people who interacted with photos of Economic Freedom Fighters*. Facebook allows the user to create such a query, but upon executing the query, Facebook states that it is currently not available. In the future, such a query will be available and yield results, as well as other queries thereby improving the social search facility within Facebook, as well as increasing the security flaws.

D. Test

The most reliable way to determine whether a user is safe from potential harmful graph queries on Facebook is to use one's own data and run queries to determine if any personal information is publicly accessible. For example, for the purpose of a test, a user A could ask a friend B, to temporarily terminate their friendship relationships on Facebook. Thereafter, A, could supply B with a set of dangerous and specialised queries that are designed to potentially return A in the results. For instance, query 12, *Photos of men who work at CSIR and live in Gauteng, South Africa from April 2014*, could be used. Such tests should be conducted periodically due to the constant change in Facebook's infrastructure.

VI. Conclusion

From the analysis conducted, it is apparent that Facebook's graph search returns many results even in cases where a Facebook account has no data or friends. Furthermore, results are increased considerably with an account with friends. The ease-of-use with the graph search simplifies numerous cyber-related privacy and security related crimes, and as the graph search grows and evolves, so will the threats.

Section IV presented the negative implications that Facebook's graph search poses to users. It was shown that the results of some of the queries can empower cyber criminals with personal information of strangers making them more susceptible to attack.

The effects that the advancements in widely used social networks such as Facebook's have on cyber security is important to note and include in awareness campaigns to help protect citizens from unknowingly disclosing personal information. Facebook's graph has the potential to be used to aid attack attempts in cyber security crime, such as social engineering.

In general, Facebook's graph search is a great tool for linking heterogeneous data and activity among people, and a great step towards the Semantic Web; the advanced web where meaning is represented and in which machines can better understand human data. However, without exercising caution, a user may be exposed to numerous types of cyber-crime such as privacy breaches, identity theft, stalking, and spam.

References

[1] A. Acquisti and R. Gross, "Imagined Communities: Awareness, information sharing, and privacy on the Facebook," *in 6th International Workshop on Privacy Enhancing Technologies (PET '06)*, ser. Lecture Notes in Computer Science, vol. 4258. Springer, 2006, pp. 36–58, Cambridge, UK, June 28-30.

[2] A.K. Al-Rawi, "Cyber warriors in the Middle East: The case of the Syrian Electronic Army," *Public Relations Review*, vol. 40, no. 3, pp. 420-428, 2014.

[3] P.B. Brandtzæg, M. Lüders, and J.H. Skjetne, "Too many Facebook "friends?" Content sharing and sociability versus the need for privacy in social network sites," *International Journal of Human–Computer Interaction*, vol. 26, no. 11-12, pp. 1006-1030, 2010.

[4] L. Caviglione, M. Coccoli, and A. Merlo, “A taxonomy-based model of security and privacy in online social networks,” *International Journal of Computational Science and Engineering*, vol. 9, no. 4, pp. 325–338, 2014.

[5] K.K.R. Choo, “The cyber threat landscape: Challenges and future research directions,” *Computers & Security* vol. 30, no.8, pp. 719-731, 2011.

[6] C. Edwards, “Ending identity theft and cyber crime,” *Biometric Technology Today*, vol. 2014, no. 2, pp. 9 – 11, 2014.

[7] B.-Z. He, C.-M. Chen, Y.-P. Su, and H.-M. Sun, “A defence scheme against identity theft attack based on multiple social networks,” *Expert Systems with Applications*, vol. 41, no. 5, pp. 2345 – 2352, 2014.

[8] P. Isenberg, D. Fisher, M. R. Morris, K. Inkpen, and M. Czerwinski, “An exploratory study of co-located collaborative visual analytics around a tabletop display,” *in Proceedings of the IEEE Conference on Visual Analytics Science and Technology (IEEE VAST ’10)*. IEEE, 2010, pp. 179–186, Salt Lake City, Utah, USA, 24-29 October.

[9] A. Labuschagne, M.M. Eloff, and N. Veerasamy, “The dark side of web 2.0,” in *ICT Critical Infrastructures and Society*, ser. IFIP Advances in Information and Communication Technology, M. Hercheui, D. Whitehouse, J. McIver, William, and J. Phahlamohlaka, Eds. Springer Berlin Heidelberg, 2012, vol. 386, pp. 237–249.

[10] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, "Towards an ontological model defning the social engineering domain," in *11th Human Choice and Computers International Conference*, Turku, Finland, July 2014.

[11] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, “Social engineering attack framework,” in *Information Security for South Africa*, Johannesburg, South Africa, August 2014.

[12] J. Parra-Arnau, D. Rebollo-Monedero, and J. Forné, “Measuring the privacy of user profiles in personalized information systems,” *Future Generation Computer Systems*, vol. 33, no. 0, pp. 53 – 63, 2014.

[13] L. Shona and M. Warren, “Security issues challenging Facebook,” in *Proceedings of the 7th Australian Information Security Management Conference*. SECAU- Security Research Centre, 2009, pp. 137–142, 1st - 3rd December, Kings Hotel, Perth, Western Australia.

[14] F. Stutzman, R. Gross, and A. Acquisti, “Silent listeners: The evolution of privacy and disclosure on Facebook,” *Journal of privacy and confidentiality*, vol. 4, no. 2, p. 2, 2013.