JAICT
ISSN 2355 1771
E-ISSN 2723-4827

JOURNAL OF APPLIED INFORMATION, COMMUNICATION AND TECHNOLOGY

Published by:
Research Center of Technology and Innovation
Directorate of Academic Research and Community Services
Swiss German University

Privacy in Social Media

Jeffry Hirawan, Itmam Al-Rasyid

Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Article Information

Received: 11 December 2019
Accepted: 9 January 2020
Published: 18 March 2021
DOI: 10.33555/ejaict.v7i1.76

Corresponding Author:

Jeffry Hirawan
Email: jeffry.hirawan@student.sgu.ac.id

ISSN 2355-1771
eISSN 2723-4827

ABSTRACT

Nowadays social networks become very common. People use social media to keep people in touch, businesses, organizations, and many more. The information you share with your friends in the social media allows them easily to keep in touch with you. However beside friends, colleges, relatives, there are many people that are interested in the private information on social media. Identity thieves, scam artists, debt collectors, stalkers, companies use social networks to gather information. Companies that use social networks for getting information about people are intended to personalize their services for the users and to sell to advertisement. In this paper we will discuss the advantage and disadvantage of using social media and what kind of information is safe to post and how to protect it.

Keywords: *Social Media, Social Networks*

1. Introduction

Nowadays social networks become very common. People use social media to keep people in touch, businesses, organizations, and many more. The information you share with your friends in the social media allows them easily to keep in touch with you. However, beside friends, colleges, relatives, there are many people that are interested in the private information on social media. Identity thieves, scam artists, debt collectors, stalkers, companies use social networks to gather information. Companies that use social networks for getting information about people are intended to personalize their services for the users and to sell to advertisement. In this paper we will discuss the advantage and disadvantage of using social media and what kind of information is safe to post and how to protect it.

2. Types of Social Networks

There are many types of social network most of them are combined elements of more than one social network.

2.1. Personal Networks

It allows users to create profiles and connect with other users. It also often involves sharing users’ information with other approved users, like gender, interests, age and many more. This type of network is for example, Facebook, Friendster, and MySpace.

2.2. Status Update Networks

This type of social networks allows users to post their status in order to broadcast information quickly and publicly to all other approved users. An example of this network is Twitter.

2.3. Location Networks

This type of network uses GPS and is able to send one’s location. Its function is to let know the location, find user nearby, and many more. Some example of location networks are Foursquare, Waze and Path.

2.4. Content-Sharing Networks

This network is designed for sharing content, such as music, photographs and also videos. The most famous content-sharing network is YouTube.

2.5. Shared-Interest Networks

This type of network allows users to share their interests with other users which have the same interests. Such as hobbies, educational backgrounds, political affiliations, etc. Examples of this type of network are deviantART, LinkedIn, Black Planet, and Goodreads.

3. What Information is Public?

Information that can be gathered from a user’s social network are divided into two types, information that is shared to users and information gathered through electronic tracking.

3.1. Information a User Shares

Information a user shares are photos, status, personal information, hobbies, etc. There can be set to public by the user or also by the social network. Here are some examples:

- A user may choose to post information as “public”.
- The privacy policy of a social network can change it at any time without the user’s permission.
- Approved users may copy and repost information, including photos without the user’s permission.
- Third-party applications that have been granted access to the social network may view information that the user or a user’s contacts post privately.

3.2. Information Gathered by Electronic Tracking

Information may also be gathered from users’ actions online using “cookies”. Information that cookies have stored: Some of the purposes of cookies may include:

- Websites the user has visited.
- Information associated with specific website.
- Building a profile around a user.

4. Who Can Access Information?

When posting information to a social network, the user probably expects approved users to be able to view it. However not only your contacts can see the information but also others, in a legal and also in an illegal way.

Legal information collecting:

- Advertisers are interested in personal information so they can better target their ads to the right people
- Software developers who use information to personalize applications.

Illegal information collecting:

- Identity thieves who steal personal information either based on information a user posts or that others post about the user.
- Other online criminals, like scamming, harassing individuals, and malware

4.1. Behavioral Advertising

Free social networks make their profits through advertising. This is often done through behavioral advertising, which is also known as targeting.

Behavioral advertising is the practice of tailoring advertisements to users’ personal interests. Social networks collect a lot of information about users, which advertisers are very interested into it. In some ways, this may be useful to the user because the advertisements they see may appear more relevant. There are some concerns about behavioral advertising, users are not aware that their information are associated with their social network profile and they are not able to view their information.

4.2. Third-Party Applications

Some social networks allow third-party applications that can interact with a social network even without being part it. Once it has the permission from the user, it allows viewing users' information, public or private, to make the application useful and also personal information.

The most typical types are:

- Games to play with contacts
- Online polls or quizzes
- Software that allows users to post into their social media profile form a phone app or web application

Most of the users allow third-party application accessing their profile without realizing the extent of the permissions being granted.
Third-party applications are able to access information that is public and also private.

4.3. Government and Social Network

The Electronic Frontier foundation (EFF) and University of California have reveals that the government use social media for investigation, surveillance and data collection. Government agencies have developed a training which teaches how to use social network information during investigations. They also use fake identity profile to manipulate the user to get into their contacts.

The electronic Communications Privacy Act allows the government to access information in social network. Social network has also been used to gather evidence of a criminal activity. For example, posting about underage drinking, sexual activities with underage, etc. can be evidence in a court case.

4.4. Some Creditors Use Social Networking Sites

Some creditors are beginning to gather information about their customers in order to sink their risks. They are gathering credit reports from social media so that they won't offer loans to unqualified customers who are unable to pay back. The decision of a creditor which uses social network to gather information is largely unregulated. The consumers do not have rights to correct or dispute information in social media, because the information are not reported to third parties.

5. Social Networks and Job Searches: Pros and Cons

Jobseekers have turned to social networks to search out for job opportunities. However, an unprofessional profile and posts with unsuitable information can destroy your reputation. On the other hand, positive and professional posts give a good reputation.

5.1. How Social Networks Can Help Jobseekers

There are a variety of ways social networks can help Jobseekers. It can increase the networking opportunities, find the right person, and also learn their behavior. For example, LinkedIn a professional network, which provide information about education status, employment history and accomplishments. It can also confirm the applicant's interest, education level, etc., which he or she represents in the application.

5.2. How Social Networks Can Hinder the Jobseekers

Companies often make its decision by what they can find about the applicant. Social networks may reveal information about the jobseekers which are unflattering. So, it is important to know what information can be seen by public. Unflattering pictures or posts could seriously affect the likelihood of getting hired. Even if the posts are set to private, there are many ways in which it may become available.

The Fair Credit Reporting Act (FCRA) is a law not only for credit reports but also to set national standards for employment screening and background checks. However, it only applies to employers using third-party screening companies. Information that employers gather are not covered by the FCRA.

5.3 How You Can Get Fired by Social Media Networks

Companies are monitoring their employees what they post on social network. Many companies have social media policies which limits the posts of their employees. Compliance Building is a website which stores hundreds of companies' social media policies in its database.

In USA some states have laws for social media posts that could damage the company and also discriminating other employees by its race, color, religion, etc. and people can contact a lawyer in the National Employment Lawyers Association if they are discriminated.

In 2010 a company called Teneros launched a social sentry service that can track employees' social media in order employees won't leak sensitive information and to protect the company's reputation.

6. Anonymity in Social Media

Social media users tend to mask their real identity. This can be done by not providing a name, and a false name. People who refuse to reveal their identity include:

- Individuals with medical conditions who want to discuss symptoms and treatment without creating a public record of their condition
- Bloggers and activists engaging in political discourse, especially on controversial issues
- Teachers and childcare workers
- Medical professionals, including mental health professionals

- Law enforcement agents, prosecutors, parole and probation officers, judges, and other court employees
- Victims of stalking, sexual assault, and domestic violence
- Children and youth
- Jobseekers

A lot of people use anonymity to shield their identity while doing illegal activities, and using anonymity they are trying to separate their online and offline identity.

In fact, it is not easy to separate online and offline identity in the internet, photos, groups, contact, and membership can still be link to specific individuals.

6.1. Laws That Protect User's Online Information

There are currently several laws that protect user's specific information in social media. Most privacy laws in the United States only protect specific type of information such as medical and financial reports. The law that protects these privacy did not protect casual information such as picture on your Facebook page.

Some rules that protect privacy online are:

- Electronic communication privacy act. Law enforcement are allowed to access data stored in the server with a subpoena.
- Children's online privacy protection act (COPA), have to limit their data collection on a certain age limit. They cannot collect data from someone who is less than 13 years old.

7. Discussion

Social media is where connect with other people. We can find people with common interest, express our opinion, and socializing. many post gossips, rumors, and interesting stories and picture for our friends to enjoy. But this may cause problem if parents or potential employer or costumer see the post. The information that we share in social media is hard to control because everyone can see it. Making your account private only helped a little since people can look what you posted through your friends account.

In social media there are 2 aspects that we need to consider:

a. The information that we share
b. The responsibilities of the companies that host our information

The information that we share may endangered people or our self. A simple status like "going to the cinema with my friends" can attract potential burglar to break in to your house since they know that you are away.

In Instagram everyone posts pictures. They post pictures of their families, friends, and themselves. We need to remember that we need to think before we share anything to Instagram because it can be potentially dangerous for us. In Instagram there are a lot of accounts that gather and post pictures of women. These pictures are inappropriate and it is posted without the consent of the owner. These accounts also provide the name of the person in the picture they posted which can be potentially dangerous for them. These pictures will invite unwanted attention of predators and other sorts of bad people.

There are no rules and laws that prevent this from happening, Instagram can block this account but there are so many accounts out there that do this thing that it has become impossible for Instagram to block them all.

We can deal with this problem by using the “private my account” function. If your account is private that mean people will need your permission to look at your post. You can allow person that you know to view your post. If you did not do this, anyone can look at your post freely and you will not know who saw it, what kind of people saw it and what are they doing with your post.

Making your account private only minimize the danger of social media, it does not solve the problem 100 percent. To avoid dangerous people, we need to think before we post anything to social media. We need to be careful the information that we share. We can know what kind of movies that a person likes, what kind of music that person likes, where does he regularly go, who are his friends, some social media even provide “check-in” feature which let you tell everyone where you at right now. People can use this kind of information to find more stuff about you. They can look for password by using your birth date; they can know that your house is empty if you use the “check in” feature regularly.

8. Conclusion

Privacy in social media are minimal, everyone can see your post and access them freely, there are no rules and regulations from the government that protecting casual information, it only protects specific types of data. People can use the information you share in the social media, and use it to uncover more information about you. You can minimalize the threat in social media by making your account a private account, so people need to ask for your permission to see your post. Secondly, we need to be careful about the information that we share or the things we post, because it can endanger us.

Reference

https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social#anonymity