

“On the Internet, nobody knows you are a dog”: A Facebook case study

Emin İslam Tatlı (tatli@de.ibm.com)

August 2009

1. Motivation

Protection of personal data is inevitable in our society. Privacy enables a person to safeguard information about himself and prevents their unintended release to others. It is a human right from legal, social and ethical perspectives. Everybody is expected to respect other's privacy. But in the digital world it has become nearly impossible to guarantee privacy due to different reasons (e.g. easy access to data, impossibility of data removal, human-relevant factors).

Name, surname, address, e-mail address, birth date, phone number, books read, groups involved, people communicated, pictures taken etc. are all personal and private information for people. They require keeping control over personal data and the danger of their misuse makes people feel uncomfortable.

In the physical world, people are accustomed to guaranteeing privacy of their personal data. They can intuitively decide *who* can get *which* of their data *when* and under *which* conditions. As an example, one would not easily give away his or her pictures to other people which they do not know. They would not easily let foreigners get to know their e-mail address and phone numbers as well. As a result, people feel in general control over their personal data.

But in the digital Internet world, controlling of privacy has become much more difficult compared the physical life. The main reasons for this dilemma are as follows:

- *Easy and continual access to data:* Personal data is easy to access, to copy, to forward; but difficult (*even impossible* [1]) to remove when it is once online.
- *Anonymous access:* Since anonymous access to data is possible, legal, ethical and social aspects are no more regarded.
- *Bad privacy approaches:* Service providers do not give enough efforts to protect privacy. They either come up with weak default protection (i.e. all data is accessible to others per default) or never consider protection at all (i.e. it is not possible to limit access to data).
- *Difficulty of privacy management:* Compared to the physical world, it is much harder to manage privacy; even it is sometimes impossible.
- *Untrained people:* People which are unaware about security and privacy management can easily cause privacy leaks.
- *Laziness of people:* Even high trained people can feel lazy to enhance their privacy since this requires following of complicated processes.

With the introduction of social network sites like Facebook, StudiVZ, Xing in which nearly all types of personal data are shared with relatives, friends and business partners, accessing personal data of other people has become easier and thus protecting privacy has become more problematic. Considering privacy risks, social network sites have started integrating different privacy protection mechanisms within their systems to help individuals to guarantee their privacy. As a common approach, they define different access groups (e.g. everyone, friends of friends, friends, nobody) representing different privacy levels and let users assign an access group to their

personal data. Even though this is a good approach in theory, there exist certain problems in practice.

In this article, we have observed the privacy aspects of the social network “Facebook” and the behaviors of individuals regarding protection of privacy.

2. Privacy in Facebook

A Facebook user can add multiple friends to his friend list and join multiple networks (e.g. country networks¹, company networks, education networks). He can share a set of his personal data (e.g. name, surname, phone numbers, address, emails, web sites, friend list, tagged photos and videos etc.) with others. The complete set of personal data shared is given in Table 1.

Facebook regulates the access to personal data based on certain access groups ranging from *everyone* to *no one*. The complete list of the access groups is given in Table 1. For each type of personal data, users can assign a group and let only those users belonging to this group access to the data. Table 1 shows possible assignments between personal data and access groups.

		Access Groups												
		Everyone	Except These People	All of Networks	My Networks and Friends of Friends	My Networks and Friends	Some of Networks	None of Networks	Friends of Friends	Only Friends	Some Friends	Only Me	No One	
Personal Data	Basic Info (Settings->Privacy Settings->Profile->Basic)													
	Profile	x		x		x	x	x	x	x				
	Basic Info	x	x	x		x	x	x	x	x				
	Personal Info	x	x	x		x	x	x	x	x				
	Status and Links	x	x	x		x	x	x	x	x	x			
	Photos Tagged of You	x	x	x		x	x	x	x	x	x	x		
	Videos Tagged of You	x	x	x		x	x	x	x	x	x	x		
	Friends	x	x	x		x	x	x	x	x				
	Wall Posts	x		x		x	x	x	x	x			x	
	Education Info	x	x	x		x	x	x	x	x	x	x		
	Work Info	x	x	x		x	x	x	x	x	x	x		
	Contact Information (Settings->Privacy Settings->Profile->Contact Information)													
	IM Screen Name		x	x		x	x	x	x	x	x	x	x	x
	Mobile Phone		x	x		x	x	x	x	x	x	x	x	x
	Other Phone		x	x		x	x	x	x	x	x	x	x	x
	Current Address		x	x		x	x	x	x	x	x	x	x	x
	Website	x	x	x		x	x	x	x	x	x			
	Emails		x	x		x	x	x	x	x	x	x	x	x
	News Feed and Wall (Settings->Privacy Settings->News Feed and Wall)													
	Social Advertisements										x			x
	Search (Settings->Privacy Settings->Search)													
	Search Visibility	x		x	x	x	x	x	x	x	x			
	Applications (Settings->Applications Settings->Edit Settings->Profile)													
	Applications you use	x		x		x	x	x	x	x	x		x	

Table 1: Facebook Privacy Matrix

¹ A user can be a member of only one country network at a time.

As shown in Figure 1 and Figure 2, the privacy settings of basic profile and contact information can be configured according to the privacy matrix.

Profile [Only Friends] [?]
 Basic Info [Only Friends] [?]
 Personal Info [Only Friends] [?]
 Status and Links [Only Friends] [?]
 Photos Tagged of You [Only Friends] [?]
 Videos Tagged of You [Custom] [?]
 Friends [Only Friends] [?]
 Wall Posts [] Friends may post to my Wall [?]
 Education Info [Only Friends] [?]
 Work Info [Only Friends] [?]

Figure 1: Privacy Settings of Basic Profile

IM Screen Name [Only Friends] [?]
 Mobile Phone [No one] [?]
 Other Phone [No one] [?]
 Current Address [No one] [?]
 Website [Only Friends] [?]
 @gmail.com [Only Friends] [?]

Figure 2: Privacy Settings of Contact Information

The privacy matrix can also be applied on news feed, wall, search and applications you use. As an example, Figure 3 and Figure 4 show privacy settings of the default application “Events”.

Box: Available (add)
 Tab: Available (add)
 Privacy: [Only Friends] [?]
 Everyone
 My Networks and Friends
 Only people at IBM
 Friends of Friends
 Only Friends
 Only Me
 Customize...

Figure 3: Privacy Settings of Facebook Application Events

Events has permission to:
 Publish to streams
 Allow Facebook to notify me by email when someone:
 Invites me to an event
 Changes the date or time of an event
 Cancels an event
 Makes me an event admin
 Requests to join an event of which I am an admin
 Posts on the wall of an event I admin
 Changes the name of an event to which I was invited

Figure 4: Settings for Additional Permissions

Privacy of photos and videos can be enhanced based on the privacy matrix as well. Figure 5 and Figure 6 show privacy settings of a photo album.



Figure 5: Album Privacy



Figure 6 : Privacy Settings of Albums

2.1. Additional Privacy Settings

In addition to the assignments based on the privacy matrix, Facebook provides additional methods for protecting privacy:

❖ Settings->Privacy Settings->News Feed and Wall->Actions within Facebook

- **Wall:** When you post on someone's wall, your mutual friends can be informed about this post if the option "Show Wall Posts" is enabled.
- **Highlights:** When you comment or like a note, a photo, an album, a video or a link or change your relationship status, these activities can be shown on your friends' home pages if the relevant options in highlights are enabled.
- **Recent Activity:** When you remove your profile information, post on a discussion board or add a friend, these activities can appear on your own wall if the relevant options are enabled. Recent activities can also be displayed in your chat conversations if enabled.

❖ Settings->Privacy Settings->Search

- **Search Result Content:** Within this option, you can set which information (i.e. picture, friend list, the link to add as a friend, the link to send a message, pages of which you are a fan) people can see when they find you by Facebook search.
- **Public Search Listing:** By enabling or disabling this option, you can control if your search would become available outside of Facebook.

❖ Settings->Privacy Settings->Applications->Settings

These are the settings that control what types of information your friends can see about you through their Facebook applications. If you do not want to share any information, you need to remove all applications you added within your profile and remove your permissions to all external applications that you may have used. Additionally, Facebook connect and beacon websites interacting with your profile can be disabled in these settings. This setting page lists your blocked applications and ignored application inviters as well.

❖ *Settings->Privacy Settings->Block People*

You can block certain people and prevent them from finding you by Facebook search, accessing your profile/other personal data and interacting with you through Facebook channels.

2.2. Bad Privacy Approaches

Even though Facebook provides many good solutions to support user privacy, there are some certain aspects that can be considered as bad privacy approaches:

- *Ignorance of User Consent:* The consent of users is a key point in privacy protection. The users should give their consent explicitly and be able to revoke it at any time according to the EU directives [2]. Facebook ignores user consent during network joins. When a user joins a network, the privacy settings are *automatically* changed and the profile and other personal data become accessible to all members of the newly joined network without asking the user for his or her consent. Actually, the user is informed about a possible change with the statement „*You are now affiliated with this network. Your profile privacy settings may have changed*“. But this is not a user-friendly method to protect privacy.
- *Unmanageable Settings for Privacy Protection:* For certain types of personal data (e.g. friend list, basic and profile info), the access group “*no one*” and “*only me*” are not supported. The minimum access group for such data is “*only friends*”. As a concrete dilemma, you can not hide your friend list from your friends. On the other hand, the access group “*except these people*” is supported for these data. But if you want to hide your friend list, you need to enter all your friends’ names within the “*except these people*” option and update this list whenever you add a new friend to your list. It is clear that this is an unmanageable option for privacy protection.
- *No prevention of tagging:* Facebook does not provide any method for prevention of tagging. That means one can not prevent others to tag him or her within their photos. This is not a good privacy approach. On the other hand, the “*remove tag*” option is supported and you can use this feature to remove the tags you do not want.

3. The weakest Chain is Human

A very critical privacy breach was experienced in June 2009. The wife of the new head of MI6, United Kingdom’s intelligent agency, published family photographs and personal details on Facebook [4]. She gave the details of where they live and work, their friends’ identities and where they spend their holidays etc. Service providers can provide the best methods for protecting privacy. But it is a known fact that people are the weakest link in the security chain and as the example shows people can often cause security and privacy leaks.

The key point for protecting privacy in Facebook (*or in general in social networks*) is that you allow only people in your friend list to access your profile and your personal data. At this point, the following question raises: “*Are people careful and sensible for accepting friendship requests?*”. We have tried to observe the answer of this question and come to a conclusion that people can easily give up their privacy.

3.1. A Facebook Case Study

Considering the fact “*on the internet, nobody knows you’re a dog*” [3], we created two faked Facebook accounts, i.e. one female and one male account. Each account contained faked personal data including faked pictures. For each faked account, we sent friendship requests to *randomly-chosen* 100 females and 100 males.

After one month we checked how many of the requests were accepted. As detailed in Table 2, the results were quite interesting. A number of users did accept friendship requests even though they did not know the request sender. More interestingly, some people sent messages asking if they knew each other *after* they had already accepted the request.

Faked User	Victim User	# of Accepted Requests/Total Requests	# of Messages sent by Victim Users	# of Sent Messages after accepting the request	# of Sent Messages before reacting to the request
Faked Female	Males	48/100	24	7	17
	Females	30/100	15	5	10
Faked Male	Males	21/100	6	2	4
	Females	35/100	10	2	8

Table 2. Total number of accepted requests and sent messages grouped by sex

According to the results in Table 2, the male users were quite careless when they got requests from the faked female user. 48% of the male users did accept the requests. 24 male users sent messages to the faked female user asking if they knew each other. Interestingly, 7 of these male users sent the message *after* they had already accepted the request. On the other hand, when the males got friend requests from a faked male, they became more sensitive. Only 21% of the males accepted the friend requests sent by the faked male user. On the other hand, we did not reply the messages. If we had replied and interacted with the victims, we believe that could increase the ratio of accepted friendship requests.

This study shows that people are not very careful regarding their privacy. They can easily become victim of social engineering and get deceived regarding the identity of their communication partner. Additionally, they are especially more insensitive for the opposite sex.

4. Summary

In the Internet, especially with the introduction of social networks, privacy of personal data is in danger. As an individual, you require to protect your privacy as you try to do in the physical life. You should benefit the privacy mechanisms provided by the social networks and enhance and update your settings according to your privacy requirements. Especially, you should never forget that your communication partner might be someone else than as you think and should release your personal data only if you become sure about the identity of the other party.

Finally, the main aspects for better privacy management in Facebook can be summarized as follows:

- Never add anybody you do not know into your friend list.
- Add a friend into your list only if you are sure about his or her identity. Name-surname pair is common for many users and does not provide enough authenticity. Analyze further for the identity by checking e-mail address, pictures, common friends etc.
- Never accept friendship requests from users you do not know.
- If you join into a network, change your privacy settings accordingly.
- Uninstall the unnecessary applications for you that are installed per default (e.g. Events, Gifts).
- Do not install any external application you do not need and consider possible risks before installation.
- Enhance the privacy settings of your applications (see Figure 3 and Figure 4). Especially enable email notifications within additional permissions.
- Enhance your privacy settings and make your personal data maximum available to your friends (see Figure 1). For your contact information, be stricter (see Figure 2).
- Enhance the privacy settings of your published photos, albums and videos (see Figure 5 and Figure 6). If required, use “*remove tag*” function to remove yourself from pictures and videos tagged by others.
- If you do not use Facebook anymore, deactivate your account.

References

- [1] “*On the Internet, Things Never Go Away Completely*”, Thomas P. Keenan, The Future of Identity in the Information Society Third International Summer School, 2007, www.cs.kau.se/IFIP-summerschool/IFIP2007POST/papers/S01_P2_Tom_Keenan_1.pdf
- [2] EU Directive 2002/58/EC on privacy and electronic communications, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>
- [3] Cartoon by Peter Steiner. The New Yorker, July 5, 1993 issue (Vol.69 (LXIX) no. 20) page 61, http://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog
- [4] Wife blows MI6 chief’s cover on Facebook, www.timesonline.co.uk/tol/news/uk/article6639521.ece