Linking social networks with virtual worlds and online games

A study of the dangers related to personal information getting in the wrong hands

Christer Persson
Abstract

The purpose of this article is to inform researchers and developers of cross-media solutions about the risks of exposing too much information about their users when they integrate social networks such as Facebook into their products. Lately online games and virtual worlds has started looking more and more towards Facebook and twitter as potential ways to increase their presence among users. This article will look at the negative aspects of doing this to help avoid doing mistakes that affects users negatively. This article will also look at some of the consequences of personal information getting in the wrong hands. Even though the majority of internet users are unaffected by their personal information being shared, it’s important to think about the few people that do get in trouble from it.
1 Introduction

1.1 Background of this article

With the increased presence of social networks, the video game industry has now started looking for new possibilities related to these. The famous game developing company Blizzard already signed a contract with Facebook and came up with a new system called Real ID for their existing online gaming platform Battle.net. Some popular games that uses Real ID are World of Warcraft, which is the most popular online game today and Starcraft II. World of Warcraft alone has over 12 million users and makes Real ID really interesting for this study. When I first heard about Real ID, I immediately felt concerned about the potential threats from online stalkers. Second Life is an online virtual world focused on people from all over the world meeting each other and creating their own content. Since I’ve been on Second Life for 4 years, I know how bad people can behave online towards other people just by standing in an area and observing their behaviour. This gave me the idea to investigate what the risks of sharing your own personal information are when integrating them into a virtual world such as Second Life. An idea of how such an integration would work would be for example your in game profile page. Here you can find a page called first life, which is basically a place to tell more about yourself if you wish. Linking Facebook to Second Life could replace this page with your own Facebook profile. Another way of doing such an integration in Second Life would be to use a similar system like Real ID, that will be explained more in detail later in this article. Linking a social network such as Facebook to a virtual world like Second Life would come with a risk of exposing users to different types of stalkers and people who wants to ruin their online experiences. With this background I came up with the following research question.

1.2 Research question

What are the dangers of exposing too much personal information in virtual worlds and online games by linking them to social networks such as Facebook?

1.3 Purpose

This article aims to inform researchers and developers of new cross-media solutions about the risks of personal information getting into the wrong hands. An example of this would be when they design a system that enables people that the users don't know in real life, to view this information. It will also inform about people's thoughts and opinions surrounding the way personal information is already being handled in existing solutions such as Facebook and Real ID.
2 Method

My goal is to study the dangers of linking social networks such as Facebook with online games with social interactions. To do this, I decided to study the consequences of sharing personal information in mainly social games such as Second life and World of Warcraft. Additionally I am also studying an existing example of Facebook integration in Blizzard's online gaming platform Battle.net, named Real ID. I have included empirical data from blogs and news websites, as I found it relevant to get information from as many different sources as possible in this study. Along with all this I’ve searched for related research through articles and books, to give me further insight on the subject.

To get a good understanding about people's perceptions of the issues with sharing personal information online, I’ve decided to interview people to get more qualitative data with the help of a book named Forskningsmetodik (Holme, Solvang, 1996). This is because I could get new interesting views on things that I didn’t think about before. This is important since there is not much information in this area to lean back on with social network integration in games being such a new and unexplored territory. I also want to be able to hear potential stories about consequences people had from too much personal information getting in the hands of the wrong people. An important thing to note is that I’ve been in Second Life for four years and that leaves me with a level of pre-understanding (Bjereld, 2002). This has influenced how my questions were constructed and will also to a degree give me an idea of what the answers to those questions will be. Without pre-understanding you can't conduct research (Bjereld, 2002). By knowing what information is especially dangerous to share, designers can take the necessary steps to prevent such information to getting into the wrong hands. Another good thing with an interview is that some explanation about Real ID might be needed in order to get the information needed from the subjects. If I had more time I would take a quantitative approach as well and do a survey, to get a better picture of how common it is for people to get bad experiences related to their personal information getting exposed.

I used Second Life to find people for my interviews and decided to focus on women because they tend to be more targeted according to my past observations in Second Life. The Subjects were not chosen because of any special reason. They just happened to be in the same area when I decided to do my interviews and I asked who had enough time to participate. I had interacted with some of them before but I didn't know if any of them had any past experiences with any type of stalker. This way I got a more fair view of how common it is to get a bad experience related to their personal information getting into the wrong hands. The subject's nationalities were, Sweden, USA, France and Australia. I did a semi structured interview with each subject based around how they handle their personal information online. Did some followup questions to get them to say more when I found that they could have more to say about the subject. I chose not to correct the spelling errors from the interviews as I wanted to show their exact words. One thing that can work against the use of interviews could be if the subjects give me answers that they think I want to hear rather than giving their own opinions. There is also a possibility to question the credibility of the information I found on some of the websites. They will however, be treated as information to strengthen my theories rather than actual facts.
3 Related Work

The following section includes research taken from research journals.

3.1 The Cyber stalker

Pittaro (2007), writes about the cyber stalker. He mentions that the cyber stalker is an extension of the traditional stalker with the difference that the person can remain anonymous. The cyber stalker is motivated by the desire to have power, control and influence over a victim. The difference between the traditional stalker and the internet stalker is that virtually anyone can be targeted. They are more inclined to target people at random. He mentions that 50% of all targets did not have any prior contact with each other.

In an example (Pittaro, 2007), mentions that with the internet, finding information about a person has become significantly easier. The stalkers can get information from either free websites that provide personal information, or go to websites where they have to pay to find out the information they can't find for free. He then proceeds with a story about a 21 year old man that was obsessed with a girl from high school that had rejected him. He paid a website for personal information about her numerous times until he found out where she lives and where she works among other things. He then made a plan to kill her and posted it on a website titled with her name. He then executed his plan and managed to kill her before taking his own life. All the information he needed he got from just knowing her name and where she was from.

Pittaro (2007), writes that the internet is particularly appealing to cyber stalkers and other online predators because they are drawn to the relatively inexpensive cost, ease of use and the anonymity it offers. He says that they can be confused with sexual predators, however not all cyber stalkers are motivated by sexual obsession. But he mentions you can't ignore how easy it is for sex offenders and pedophiles to also use the internet as a virtual playground.

McFarlane and Bocij (2005), categorizes Cyberstalkers into four different categories.

- Vindictive cyberstalker: Tries to victimise their targets. Mental health problems common with a great chance it will turn into offline stalking.
- Composed cyberstalker: Wishes to cause distress in their targets. No mental health problems.
- Intimate cyberstalker: Wants go get intimate with their targets.
- Collective cyberstalkers: A group of two or more who harasses a target.
3.1.1 The victims of Cyber stalking

Pittaro (2007), writes that it's usually males harassing females on the internet. However the cases where females are the offenders it turns out that it's usually ex-partners that are the victims. When females harass other females it turns out that it's usually to form an intimate relationship with the target. Males are more inclined to harass random people instead of people they know as opposed to females who usually harass people they've been in contact with before.

3.2 Companies and personal information

Camenisch et al. (2005), mentions that it's a common misconception that people voluntarily give away their personal data. Instead they give it away due to lack of alternatives. People often give away information cause they have no choice but to fill in all required fields to use a certain service or buy a product online. Often the information that is filled in is more than what is actually required. A big problem with this is that all this data can be stolen by hackers. A recent example of this is when Sony got their Playstation network hacked and over 70 million users got their personal information stolen (Daily mail, 2011).

3.3 Behaviors vs attitudes

Joinson, Reips, Buchanan and Schofield (2010), mentions as a result of their first study that even though people expresses privacy-concerned attitudes their actual behaviour is not always reflecting their attitudes. Their second study showed that that privacy and trust however has a symbiotic relationship. If a user doesn't trust a company they are usually more careful when dealing with them.
4 Empirical investigation

In this section, relevant data from blogs, newspapers and company websites has been gathered along with my own interviews from Second Life and screenshots of Real ID.

4.1 What is Real ID?

Real ID (Blizzard Entertainment, 2011), is Blizzard's new way for people to connect with each other through their online gaming platform Battle.net. The way it works is that two people have to mutually agree to become Real ID friends. Once they did this they can see each other online in any Battle.net game. Their real life name is displayed as well as their in game activity.

Another option for Real ID is to add your Facebook friends. All the players need to do is press a search button and they get all their Facebook friends with a Battle.net account listed. However, anyone can choose to not be shown in the search results.

Another feature that Real ID adds is the option to view friends of friends, much like Facebook do. A player can right click on a Real ID friend's name and select view friends. He will then see a list of all his friends and if he wants add them to his own list. In this list the real life names are shown as well.

Real ID also allows people to broadcast a message to all Real ID friends as well as see them online on any character in any game and chat with each other across different games. There is an option to set your status to away but you can never hide your online presence. The add Facebook feature and friend of friends feature can both be toggled off on the account management web page for Battle.net. There is also a parental control feature if parents wants to shut off Real ID for their kids on this page.

![Image of Real ID interface]

*Figure 1: This is the interface where you add a new friend to Real ID.*
4.1.1 Real ID in forums

Blizzard originally planned to have Real ID in forums. The real life name of the users was shown instead of your online nickname in an attempt to make people behave better. However this lead to a wave of complaints and Blizzard was forced to exclude Real ID from their forums (Gamasutra, 2010).

4.1.2 Example of Real ID gone wrong

Here is a story from a parent that calls herself KellyX (Voodoo Extreme, 2010) that wrote this on the official US World of Warcraft forums.

It’s a nightmare that blizzard even thought this was acceptable on any level... The parental settings are almost nil. I decided it would be okay if my oldest son (16) was able to decided who he added for himself. He added his guild leader and I saw no problem in this matter. He added his older sister (24) and added me.

My daughter is now in the process of opening a ticket (8 day wait minimum) while trade chat runs rampant with her home address (thankfully not correct as she put it...), phone number, and real name.

How did this happen?

The guild leader decided it would be fun to tell people her name because she was a female. From Monica xxxxxxxx and a quick Facebook and or Google search they pulled up her life story and spammed it across trade.

Not 24 hours after it’s release and my mistake to allow a 16 year old to add his sister and guild leader on Real ID *Really bull%#!* already she’s getting death threats and "pick up lines" on her cell phone (partly her own fault for having it on facebook...). Whitebooks (phone info), Google, Skype and Facebook. All you need is a name and a potential region to start looking and this happens.
4.2 Consequences of real life information being exposed


The first blog (nyxofsl) exposes a lot of women and if available their real life name along with nude pictures they gave to their boyfriends in Second Life(SL). There is also random people being harassed in different ways. The person on this blog clearly posts anything he can get his hands on to hurt people. This blog was shut down during this study. This blog fits into the Composed cyberstalker category (McFarlane and Bocij, 2005), since it looks like it’s an individual from the way the blog posts are written.

The main purpose of the second blog (thelistsl) is to give out as much real life information about people as possible. They have a check list of user names in SL that they want to find information on. Most of the names are already crossed over since they got the information they wanted on them. The information on thelistsl included are, name, address, phone number, occupation, family members, IP, internet service provider and other specific information about what the person do in their spare time. Basically any information they can get their hands on is posted on this blog. This blog fits into the Collective cyberstalker category (McFarlane and Bocij, 2005) as it gives a hint of a group effort from reading it.

4.3 Voices from Second life

These are my interviews from Second Life with notes between each questions to explain further my thoughts of why I asked those questions. I also chose to put some notes between each subject’s answer to make it easier to understand, since they were using terms that is common in Second Life and World of Warcraft.

What are your thoughts about linking social networks such as facebook to virtual worlds and online games? What positive/negative aspects do you see related to that?

Jenny:

I try not to think about it at all. Personally I get annoyed wit all the suggestions of linking this to that. I have asked others what they think about it and most seem to think it’s very handy. I had Facebook a few years but I left it, didn’t feel sound. To me personally then; I feel chased by it and I know that many people try to keep track of their “friends” and the whole networking idea is very stalkerfriendly. Also it allowes for third parties i.e. providers and sponsors to surveill and angle the advertise ments etc. On the plus side, thats obvious, it can be a handy tool to keep track of eachother.

Jenny thinks that it is stalker friendly and allows for third parties to surveil more. But thinks that it is a handy tool to keep track of each other.

Manon:

I see no benefits to that. If I want to exchange RL info I can eventually anyway.
Manon has a more negative view on it and thinks that if she wants to exchange real life information she can do it her own way anyway.

Nikki:
well there is already SL facebook pages ....I think if the person posting it is comfortable doing that, then fine. I however have concerns with facebook's constant changing of personal info. privacy setting. basically I don't trust facebook....soon they are doing a face recognition program..I don’t like the big brother aspect of facebook especially when the point of SL is to have a second life of anonymity if one so chooses. of corse face recognition is for rl photos only...but still it's a slippery slope. it would be a bad partnership in my opinion. if people want to do a sl facebook page they already have that option.... I don’t like what facebook has become. which is why I refuse to be on it. I deactivated my acct...they don’t let you delete it which is another reason I don’t like facebook at all.

Nikki is concerned with the constant changes on Facebook and says she doesn't trust them. She has a similar view on Facebook as Jenny as they both seem to have left it for the same reason. She mentions it would be a bad partnership to link Facebook with virtual worlds. Also mentions that people already use Facebook to create a page for their in game avatars in Second Life.

Ophelia:
well I think it already happens to some degree. People in SL make facebook profiles for their avatars and keep in touch in that way, also I follow the release of games by liking them on facebook etc. i think most people want to keep their online time seperate as its a way to escape RL. It really depends what they do in virtual worlds and how much privacy they are willing to give up. well positive would be to get more rl friends into it, negative would be that I dont want all my real life friends and family know what i get up to in my virtual life hehe.

Ophelia mentions just like Nikki that people create pages for their avatars on Facebook. She mentions that she thinks most people on Second Life wants to keep their real life separate from Second Life. A positive thing she can see with linking Second Life to Facebook would be to get more real life friends into it. She does however, not want all her friends to know what she is doing in her virtual life.

Rubi:
no. i dont want poeple here to know me irl. only select people.
theres loads of weird people in SL ex. (name is censored)

I had to censor a name here as I don’t want to hang out individuals in this article. Rubi mentions that she only wants select people to know anything about her in real life. She mentions there are a lot of weird people on Second Life and mentions the avatar name of one.

I asked the next question as a test to see if they took notice when they were asked to give up personal information, when installing a Facebook application.

When you first install an application on facebook, do you remember what you see before you start installing it?

Jenny:
yes i remember it vividly. installing an application gave me a brand new application.

Jenny gave a sarcastic answer since she couldn’t remember what happened.
Manon:
No.
Manon did not remember what happened either.

Nikki:
it links with all your ‘friends’ gets their info and such

Nikki was the only one that remembers and that might be one of the reasons she stopped using Facebook.

Ophelia:
ummm not sure... i havent installed a new app in ages

Ophelia did't remember, but there is a possibility she would if she had installed an application recently.

Rubi:
hm no lol

Rubi didn't remember either.

I wanted to know if they had any problems related to them sharing personal information as a base for this question.

Did you ever have any problems related to your personal information being shared online? Do you know anyone else that had issues with this? Explain?

Jenny:
it has happened a few times but related to FB, there was a guy who stalked me and snooped around my FB friends casually asking about me and such. Also seing my RL adress and sending strenge letters. i met him on a 3d chat called worlds.com. we were both active on a web radio channel. then through mutual friends we had some contact even in SL.

Jenny mentions a stalker who she met on a virtual world named world.com which is similar to Second Life. He then proceeded to stalk her on Facebook and Second Life.

Manon:
Yes. And btw; if I’m asked for personal info by an online company, I lie. It happened on Guildwars. Both my sister and me played it, on two different accounts. We used this thing called ‘guildspeak’, which works like voice. My sis often did missions and battles with this guy from the other side of France. Was just innocent, not even flirting. One day she was in a shop in the village, a guy is talking to the elderly shopkeeper. She recognises his voice, he’s asking her if she knows two sisters living together nearby, musicians. Luckily, shopkeeper had enough sense to say she didn’t know... And Dee stayed in the back of the shop until he left. The neighbours’ sons slept over the rest of the week, it was scary. the guild did have a forum, so maybe he found us through the IP. So I don’t do fora anymore, nor speaks. I didn’t like guildspeak anyway, or teamspeak. It was just guys going ‘AAAAH DAMMIT”, ”MERDE!” and drama. I know of one other person who had something similar happening, in SL. He got a restraining order. Against the guy stalking him. The guy was bi-curious, his wife didn't know. And his 'SL friend' thought it was more. I don’t know how he found out the guy's location. voice sends a constant IP to the SL server which is - I am reliably informed - about as easy to crack as a cereal box.
Manon explains that she lies when she is asked about personal information from companies. She then explains how her sister met a person on an online game named Guildwars, which is similar to World of Warcraft. That person later sought them out in real life by asking around about them in the village they live. She also talks about a friend who had to get a restraining order against another guy who stalked him. In both cases she thinks their location was found through their IP number.

Nikki:

ha! oh yes. well, i've had people on sl try to hack/crash me and many others...most friends of mine here have had experiences ...or they give out personal info and get grieved. i see it happen to people new here. i hear them blathering about all their personal info then they are surprised when someone messes with them. i’ve encountered a couple real nasty ones. the beauty of sl is you can delete that acct and move on if you so choose.

Ophelia:

to a degree yes, i dont share it in virtual worlds..but i buy stuff online and i dont mind if corporations have it etc. well i learnt that giving too much real life info can lead to some people acting a bit...stalkerish lol especially if they live in the same city as me so i tend to avoid that.

Me:

Know anyone else that had problems?

Ophelia:

yep, lots of my female friends. some incidents irl, but thats only because she was stupid enough to meet the guy.

Ophelia didn’t mention a specific situations. Only that some guys tend to get a little too close when given real life information. She also mentions a friend who had a real life incident.

Rubi:

on facebook no, belle has had harrassment problems on SL recently. but i have my fb all private no one can see it unless im friends. Well she gave him her phone number and now he texts her all the time. he used to text her, message her on msn and facebook nonstop. he would ask him to leave her alone he wouldn't. she had to create a new character he doesn't know, delete him from msn and she tried blocking him from calling her.

Rubi mentions her friend had a problem with a person that had her phone number that wouldn’t stop messaging her even when she tried to block the phone number.

I asked if they would like to have the ability to delete any information about themselves that can be found on the internet in case some interesting answers could come out of it.

If you could, would you like to have the ability to delete any information about yourself on the internet?

Jenny:

oh absolutely. well no haha maybe not ALL. some things are related to things I have done in publik, like things i have published on national media. but it would feel nice to have other things untrackable. i imagine a future hobby for many will be to spy on their ancestor's doings online haha.

Jenny gives the impression that she only want to have the ability to remove embarrassing information about herself online.
Manon:
Absolutely. But there’s always backup. Because the internet doesn’t exist.

Manon hints that having the ability would be impossible since there is always a backup somewhere.

Nikki:
yes. I think we opened up a pandoras box by having things so unregulated. I’m not for censorship mind you, but having no rules makes all the sociopaths have a safe place to play....so to speak.

Nikki wants more regulations of how information is handled on the internet.

Ophelia:
hmm ive googled myself and havent found anything bad lol but yes, if something was posted id pay someone to fix it.

Ophelia is ready to pay money if something she bad about her was found through Google.

Rubi:
es. i would like to delete pretty much everything that comes up in google.

Rubi would like to be able to delete anything that is found about her through a Google search.

I finished the interview asking about their thoughts about Real ID. In some cases I had to explain how it works.

What’s your view on Real ID?

Jenny:
that allows me to expose people who arent aware that i even can. totally insane. i venture it wouldnt be very popular. the reason people hook up like that is probably for the gag and the gadget, SL is so full of that already that i can’t see that they would be appealed. besides, SL users seem to me rather aware the hazards and mostly rather protective of their real identities. That might be because SL is so real life like as it is.

Jenny mentions that she thinks it enables people to expose users that is not even aware of it. She then mentions SL is so filled with with gadgets already so she can’t see why a feature like this would be appealed. She also mentions SL users seem rather aware of hazards.

Manon:
Sucks.

Manon didn’t have much to say about this, other than that she didn’t like it.

Nikki:
is it an option. i mean can you opt out of that. that would be hell on sl.... that’s different if it’s an option....sl is too dangerous to have rl names. you have way too much drama on here. well, i think if you choose to do it fine..but you should never have your rl info compromised if you want to play anonymously.

Nikki was concerned that people could get their real life information compromised if a system like Real ID was brought into Second Life.
Ophelia: 
i think its good they removed the forum issue, ie. showing your real name in posts... but i dont mind having it otherwise.. its easier to keep track of my rl friends.

Me: 
Are you aware that you can also see the friends of your friends?

Ophelia: 
nope that I didnt. well its good i no longer play then, that would annoy me.

Ophelia likes the idea of keeping track of friends easy. She didn't know that you could see the friends of your friends and that concerned her.

Rubi: 
i dont like that. they can see friends that dont play wow?

Me: 
yes

Rubi: 

oh yeh i dont like that. i wouldnt like it in second life i would probally complain.

Rubi said that she would most likely complain if a system like Real ID is in Second Life.
5 Results

5.1 Analysis of interviews

From the interviews I came up with the following conclusions. Sharing your personal information can be quite dangerous if you happen to do it to the wrong person. All of the subjects had an experience to talk about, either about a close friend or themselves. Nikki mentioned that new people in Second Life tend to easier give out information about themselves.

When I explained the features of Real ID the general opinion was negative towards being able to see the friends of your friends. Ophelia did play World of Warcraft before and she found it as a neat way to get in touch with your real life friends. She did however not like the ability to view your friend's friends list when I asked if she knew about that feature. An important thing to notice is that she didn’t know that the friends of her friends could see her name. She also mentioned a forum feature which was removed. Blizzard intended to show the real life names of everyone that posts on the official forums, but it was removed due to a massive amount of complaints.

On the question about integration of Facebook in virtual worlds they were generally negative and felt that Second Life should be kept separate from real life. Nikki and Ophelia mentioned that some people makes profiles for their Second Life avatars on Facebook and Nikki said that it is fine for them to do it if that is what they want.

Only Nikki seemed to have taken notice that the company in charge of an application on Facebook asks for access to all your personal information before you can install it.

Everyone wanted the ability to delete any information about themselves online. Rubi and Ophelia mentioned things that comes up in google which can, if you have a unique name be a very easy way to find information about someone if anything comes up in the search. Symantec (2011) did a survey where 57% of internet users wants to be able to delete all their personal information online with a simple click.

5.2 The presence of offenders online

From the interviews and the two blogs I presented it is clear that cyberstalkers is not an uncommon occurrence in Second Life. thelistsl has posts with 30 different people and real life information is being presented in all of these. Additionally they have a check list of people they want to get information on. nyxosfl was aimed at hurting people as much as possible and while not as much real life information was presented. It did have some, along with naked pictures and chat logs. From the interviews Jenny revealed that she had problems with stalkers related to Facebook. The post from the Blizzard forums showed that the problem with offenders exists even in World of Warcraft, where the guild leader got hold of a woman’s real name through Real ID and posted it in the public chat channel.
6 Discussion and conclusions

While integrating social networks to a game or a virtual world can bring a lot of positive things where friends can more easily connect with each other, there are also a few dangers that needs to be addressed. If we take a look at Real ID I have listed a few positive and negative aspects of it.

Benefits of Real ID:

1. Easy to find and add people you know to your friends list.
2. You can see what your friends are doing and can see if they are busy or not.
3. You don't have to add all of their in game characters to see if they are online.

Potential problems with Real ID:

1. You see the real names of players.
2. You see the real names of your friend's friends.
3. A lot of kids play these games and their parents may not have knowledge about Real ID.
4. Features are enabled by default. Have to log on a web page to disable them.
5. No toggle to hide your online presence.

Since we established that dangers do exist and can be quite common when you interact with other people online, I think a better solution for Real ID would be to have all the features disabled by default and then have to enable them one by one. Take for example the display of your real name. I would like to see a toggle to enable to show it to your friends only. Another toggle to enable your friend's friends to see your name. This way it is more like an individual gets a choice to get a feature rather than a choice to remove a feature. This makes you more aware of what you do. Personally I think the positive aspects of Real ID is a good way to keep in touch. But it needs to be better planned. One could argue that if the features are not enabled by default the system would work in a bad way. However if you made an interface for enabling the features once you first log in to your game, everyone would be able to set it to their own preference. This would also give people more insight to all the features of Real ID, as it is concerning that Ophelia who used Real ID before didn't know that her friend's friends could see her real name. A user named Lissanna (Restokin: Lisannas blog about Warcraft druids, 2010), writes this in her blog about Real ID and it addresses the same concerns that I noticed.

Unfortunately, it's not just YOUR friends that can see all your personal info. It's also the friends of your friends. If I invite someone to be my friend, and they have 100 friends, all 100 of those friends can see my RL info, and that makes me very uncomfortable. So, I'll mostly be waiting & hoping that they add more privacy options into their system in the future. If they gave us the option to disable friends of friends, then I'd like the system a lot more. Until they implement privacy options into their system, I'm going to keep my friends circle limited.
In Second Life, people already share information to each other when they feel that they can trust the other person. New people tend to be less careful as Nikki mentioned and is something that I’ve also noticed when interacting with them in my past Second Life experiences. I think more clear information about the dangers that exists could help new users become more careful. Since second life is only one platform and not across more than one game, I see no real benefit of introducing anything such as Real ID. In fact it could be more dangerous since new people do tend to be less careful before they got some experience. The purpose of Second Life is also about meeting new people and interacting with them. In a game like Starcraft II or World of Warcraft, it is more a much common occurrence that users are hanging out with their real life friends playing a game together. In this case an easier way to find people who already are your real life friends could be beneficial.

I can see a benefit for companies to make a connection to another company with a larger user base for the purpose of getting more users to their own product and vice versa. However I think it is important to have a system that protects the customer as good as possible. I can think of an issue where a company might value profit above customer safety. An example of this is what happened recently with the Playstation network getting hacked. It was revealed that they knew about the weakness in their security and they did nothing about it (Businessinsider, 2011). Some companies are also interested in gathering more personal data from users out of a business perspective, as (Camenisch et al. 2005), mentioned when companies make people give out more information than they actually need to. In that sense a business relationship where a company makes a deal with a social network could be more than just about linking their product with it. It also means they could possibly get access to a lot of personal information that they otherwise wouldn't get access to.

Blizzard has a reputation for being a company that always brings quality games to their customers. As (Joinson, Reips, Buchanan and Schofield, 2010), mentioned, privacy and trust is in a symbiotic relationship. Because of this, Blizzard might get more trust from their customers concerning Real ID, compared to a company that is known for less quality products.

If a cyberstalker in any way gets interested in another person, a name can be enough for more information getting exposed, just like what KellyX (Voodoo Extreme, 2010), described in her forum post. Especially if the name is somewhat unique. This means companies needs to be extra careful with how they handle personal information. A user called natalie (Metafilter: Community weblog, 2010), describes in a forum thread about Real ID, how much harassment she and the other females she knew on World of Warcraft, had to put up with by males once they discovered they were females. Since people's behaviours doesn't always reflect their attitudes (Joinson, Reips, Buchanan and Schofield, 2010), they might use certain features without giving it much thought. My suggestion is that a feature that displays real names or similar data needs to be off by default if there is any risk that people you don’t trust is able to see it. That way it is up to each person to make a choice if they want to take the step to expose themselves further.
References


Accessed 2011-05-25

Accessed 2011-05-25


Accessed 2011-06-17

Accessed 2011-05-25


Accessed 2011-05-25
Metafilter: Community weblog. (2010) *But my name really is Deathblood Blackaxe*  
Retrieved from  
http://www.metafilter.com/93492/But-my-name-really-is-Deathblood-Blackaxe#3171434  
Accessed 2011-05-25

Pittaro, M L. (2007) *Cyber stalking: An Analysis of Online Harassment and Intimidation*  

Restokin: Lisannas blog about Warcraft druids. (2010). *Real ID: Do you trust the friends of your friends?* Retrieved from  
Accessed 2011-05-25

Accessed 2011-05-25

Voodoo Extreme. (2010). *Is Blizzard’s Real ID Safe, Or A Playground For Sexual Deviants?*  
Retrieved from  
Accessed 2011-05-25