GAMING CONSOLES AND PERSONAL INFORMATION: PLAYING WITH PRIVACY

The way we play online games has changed radically in the past decade. As most of the software and consoles have added a network or multiplayer dimension, we can now play with others next door, or around the world.

However, in order to enable multi-player experiences and administer a network of contacts and interactions, companies need to collect more personal information from consumers. It is also common now for profiles within gaming networks to be tied to wider online social network sites.

And while chasing high scores and questing may be the name of most games, privacy considerations shouldn't be an afterthought. As with any other online activity, how information is collected, shared and used by industry should be taken seriously.

You might ask - what kind of personal information is collected through online gaming? The answer is everything from names, addresses and credit card information for billing purposes, to email addresses and IP addresses, down to feedback rankings from others, digital images and personalized profiles.

The following are some FAQs on online games and privacy, followed by some general information and advice on how to protect your personal information while playing online.

Frequently Asked Questions

Why do online games collect personal information from gamers?

Providing personal information is often a requirement to access online gaming services. Usually in order to create an online account, gaming companies require a user's name, mailing address, email address and date of birth. Companies will often collect some geographical information for the purpose of finding the nearest gamers online to play with and to find the closest gaming server.

For online gambling games, gamers are also asked to confirm that they are aged at least 18 or older in jurisdictions in which the minimum age for gambling is 18. However, in order for individuals to wager actual money, gamers need to make a deposit and provide financial information to arrange for payment.

Why do I need to give credit card information?

Many gaming networks operate tiered services. In other words, some services or functions are available to you for free, while others require payment. Just as a credit card is needed to shop online, you often need one to play certain games or access certain services through your console.

As with any use of a credit card for Internet purchases, you should check your statements regularly and contact the gaming company or console service immediately if there are transactions you are unsure about.

Can I set my own privacy controls?

Yes. But depending on the kind of game you'll play, there may be more (or less) choices to make. In others words, the choice given to gamers around privacy controls depends greatly on the particular gaming platform, companies involved and features of the game itself. For simple, single-player games there will only be limited collection. Meanwhile, large multi-player environments will involve considerable personal information - including preferences around communication with other gamers.   As a result, some platforms may offer exhaustive and detailed controls, whereas others may provide only one or two choices.

Are there trade-offs for stricter settings?

There may be. For instance, in more sophisticated gaming environments, privacy settings can often be set very restrictively so that, for example, *no one* can see your profile or personal details except the game company itself. Because this level of security is not very conducive to multi-player gaming or the social aspects of the online experience, many gamers are less restrictive. They allow their profile to be seen by other individuals they know who use the same gaming system or console.

How does my gaming profile link up with other networks?

Just as gaming consoles and networks have added functions like reputation ratings, chat and personal profile pages to their systems, they also let gamers tie their gaming activities to other social networking sites. This means gamers can update their social site status and messages from within the game itself, without having to use a different computer or mobile device.

Why do companies link gaming profiles to other networks?

The idea is to allow gamers interested in playing online with friends to be able to notify them easily when a game session is about to start, regardless of the time or their location. While convenient, if you choose to use this feature to synchronize messages from other sites, you should read the associated privacy policies and user agreements carefully.

Where can I find the privacy policy and more information?

When you register for an online gaming service or with a networked console for the first time, you will usually establish a profile of some kind. There is usually an online interface or form that will allow you to set some personal preferences for the particular game system you are about to use. Privacy settings are usually presented at this stage.

The privacy policy is generally provided for review on screen or as a hyperlink to follow.The other point at which you may decide to review the privacy policy is when you set-up features for a console or device to connect with a wireless network.

Privacy policy information can be very helpful for finding out what information is gathered through the game console, where that information goes, how it gets used and who to complain to if there is a problem or to ask if there is a question.

Can people impersonate me online or take over my account?

No gamer wants their account to be taken over and companies actively try to minimize this risk. But whenever there is personal information used to establish a virtual presence or online identity, there is risk for abuse. There have been some high-profile cases where online gaming accounts have been taken over or blocked by virtual competitors, for example.

How can I safeguard my profile?

Given that personal information or financial details may be part of many gaming profiles, it is best to use:

- strong passwords;
- HTTPS (Hypertext Transfer Protocol Secure), a web application option which will encrypt personal information and in-game communications (where the option is provided);
- restrictive privacy settings, and
- minimal personal information of a sensitive nature (for example, avoid sharing personal information like your home address, and school or work-related details).

If permitted in a game's terms of service, you may also wish to adopt a pseudonym or nickname.

Who can see my profile and list of friends?

Each console system or game company will have different privacy defaults and options. These settings and the way you use them will determine how much information another user can see about you and your contacts.

That said, when you establish and use contact lists and online friends' information, you should also be aware that you may end up exposing the personal information of other individuals, if you do not manage your own privacy settings carefully. Because profiles are like online business cards, they are easily traded, and other people's information can often be exposed with a single message.

Who else do game companies share my personal information with?

The potential scope of disclosure from gaming profiles to various third parties is quite broad. Personal information is disclosed by gaming companies in order to comply with law, monitor disruptive behaviour, resolve service problems, further game development, ensure payment, allow communication between individual gamers or provide participants with advertising and promotional information.

The list of third parties may include: individual programmers under contract (anywhere in the world), financial institutions, online hosting or distribution services, call centers for technical and gaming support, Internet Service Providers, researchers, advertisers, marketers, and law enforcement and other state agents.Gamers should make sure the console company or game developer have set out specific terms about accountability and safeguards for personal information in their Terms of Service agreement. These are important to have in place whenever disclosures of personal information are made.

Seeking consent and/or providing notice to consumers is also very important. Gamers should also take note if a company contact is specified.

Some gaming companies state that they do not take responsibility for the personal information transferred to third parties. Their privacy policies may state that they cannot guarantee a comparable level of protection while the information is being processed by a third party anywhere in the world. To date, most gamers have limited knowledge about the potential scope of disclosure of personal information to third parties.

Who else can access my in-game communications?

Once a personal account is established within a gaming network and a profile is posted, it is a general feature to allow registered gamers to send messages or even chat live with others playing the same game. For certain mobile consoles and games, this element of the game is one of the most popular features. This can be done through a messaging system like email and chat, or via a special headset (using VOIP, or voice over Internet Protocol) much like a phone, or even within the game itself between two or more gamers.

At the same time, these communication functions are not critical to most game play. Privacy settings should allow gamers to block certain other gamers or restrict these functions entirely if there are problems. Most services also encourage gamers to report incidents immediately if another user is harassing or abusing other gamers.

Do I need to use a social network to play games online?

A relatively new development is games connected with social networking sites. Game developers create gaming applications that can be activated by gamers when they are signed onto their social networking accounts.

When individuals identify themselves for the purpose of online gaming they may do so:

- directly through a social network account,
- through a gaming console profile set up to connect with a social network, or,
- by synchronizing profiles from one online service affiliated with a gaming service.

Some personal information posted by gamers on their social networking account or profile may be used by a game operator in order to log them into a game. In other words, a gaming company may be able to collect personal information about a player from the social networking website on which the game is being played.

Privacy and Gaming Online

Statistics

According to the Pew Research Center, more than half of US adults aged 18 and older (53%) play video games and about one-in-five adults (21%) play every day or almost every day. Recent public opinion research indicates that, in the North American marketplace, something approaching 97% of teenagers play video games.

Data linking, profiling and data mining

Personal information collected by gaming companies is often used to determine the kind of gaming content that a player might be interested in, to assist advertisers in targeting their in-game advertising, or for player match-up services (to find gamers with similar skills or play against another gamer nearby). This data may be in the form of "aggregate" information.

On its own, aggregate information describes the habits, usage patterns, and demographics of gamers as a group, but does not describe or reveal the identity of any particular user.

A wider privacy concern arises when game profile data within one platform or online context - such as console warranty filing or network registration - is linked to personal information in another context like the user name and password from a webmail account. Gamers do not always realize how linking data of this type for convenience, across platforms and contexts, makes personal use profiling much easier.

Consent

In Canada, gaming companies need to obtain meaningful consent of the individuals playing their games if personal information is handled. This can be challenging when it comes to children who play games online. Many adults don't understand what's happening behind their computer screens – we certainly can't expect children to fully appreciate how their personal information is being collected and used.

Parental control and valid consent from children and youth are one of the main privacy issues with online games. Some companies recommend that minors ask their parents for permission before sending information about themselves over the Internet. After registration the parent has options to control his/her child's access to content and ability to chat with other account holders.

Retention of Personal information and Deleting Gaming Accounts

Some privacy policies issued by gaming companies have no provisions regarding data retention, deleting personal information or deactivating accounts. This means that gamers who no longer wish to continue playing a game online may 'close' their account, but still have significant amounts of personal information remain both online and with gaming corporations.

Canada's private sector privacy law says companies must ensure they have proper methods in place for disposal of personal information they no longer require. Organizations are required by law to put in place such data retention policies.   For more information on companies' obligations, please consult our website.

Additional reading and resources

- Duranske, Benjamin and Bloomfield, Robert J. "Protecting Children in Virtual Worlds without Undermining Their Economic, Educational and Social Benefits (2009). Washington and Lee Law Review, Vol. 66, 2009. URL: http://ssrn.com/abstract=1488165
- Media Smarts – Game tips for parents (2011) URL: http://mediasmarts.ca/blog/game-tips-parents
- Pew Internet & American Life Project, "Video Games: Adults are Gamers Too" (2008) URL: http://pewresearch.org/pubs/1048/video-games-adults-are-gamers-too
- Regan, P. and V. Steeves (2010). "Kids R Us: Online Social Networking and the Potential for Empowerment" from *Surveillance & Society* 8(2), pp. 151-165. URL: http://www.surveillance-and-society.org/ojs/index.php/journal/article/viewDownloadInterstitial/kidsrus/kidsrus

For more information, please contact:

Office of the Privacy Commissioner of Canada
Place de Ville, Tower B, 3rd Floor
112 Kent Street
Ottawa, On
K1A 1H3

Toll-free: 1 (800) 282-1376
Tel: (613) 995-8210
TTY/TDD (613) 992-9190
Fax: (613) 947-6850

www.priv.gc.ca

Follow us on Twitter: @PrivacyPrivee