

## **An empirical evaluation of the compliance of game-network providers with data-protection law**

**Karin Leichtenstern, Nikolaus Bee, Elisabeth André, Ulrich Berkmüller, Johannes Wagner**

### **Angaben zur Veröffentlichung / Publication details:**

Leichtenstern, Karin, Nikolaus Bee, Elisabeth André, Ulrich Berkmüller, and Johannes Wagner. 2011. "An empirical evaluation of the compliance of game-network providers with data-protection law." In Trust Management V: 5th IFIP WG 11.11 International Conference, IFIPTM 2011, Copenhagen, Denmark, June 29 – July 1, 2011; Proceedings, edited by Ian Wakeman, Ehud Gudes, Christian Damsgaard Jensen, and Jason Crampton, 149–64. Berlin: Springer. [https://doi.org/10.1007/978-3-642-22200-9\\_13](https://doi.org/10.1007/978-3-642-22200-9_13).

### **Nutzungsbedingungen / Terms of use:**

**licgercopyright**

Dieses Dokument wird unter folgenden Bedingungen zur Verfügung gestellt: / This document is made available under the following conditions:

**Deutsches Urheberrecht**

Weitere Informationen finden Sie unter: / For more information see:

<https://www.uni-augsburg.de/de/organisation/bibliothek/publizieren-zitieren-archivieren/publizieren>



# An Empirical Evaluation of the Compliance of Game-Network Providers with Data-Protection Law

Thorben Burghardt<sup>1</sup>, Klemens Böhm<sup>1</sup>, Markus Korte<sup>1</sup>, and Simon Bohnen<sup>2</sup>

<sup>1</sup> Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany  
`firstname.lastname@kit.edu`

<sup>2</sup> University of Regensburg, 93053 Regensburg, Germany  
`firstname.lastname@jura.uni-regensburg.de`

**Abstract.** Game consoles have become ubiquitous, not only for gaming but also as media servers, internet gateways etc. In combination with online networks, consoles feature online gaming in an unprecedented fashion. To participate in the networks and to personalize the services offered, the providers collect, process and forward personal information. This puts user privacy at risk. In this work we analyze the privacy policies of the online networks Playstation-Network, Xbox-Live and Wii, the three major providers. More specifically, we test the compliance of the policies to the current legal situation. We also evaluate if the providers fulfill the fundamental right of a user to obtain information on him. Our results are that all providers commit several violations, and in many cases their practices are not transparent.

## 1 Introduction

Today, game consoles have become ubiquitous. They are highly versatile and not limited to high-performance game playing as such, but feature surfing the Internet, acting as Media Servers [1] etc. Online networks, for multiplayer games in particular, have become popular. Users playing against each other register at such game networks, normally with their names, email addresses, age information, a gamer tag etc. (*inventory data*). The network then manages user authentication, payment, matching similar users for online sessions etc. (*usage data*). The console vendors Sony Playstation, Microsoft Xbox or Nintendo Wii offer such networks. Network providers also exchange information with social network sites (SNS) [2]. Further, network providers run shops and can store interests in products, purchases, shipping address etc. Thus, network providers can create comprehensive user profiles. This puts user privacy at risk.

It is not only the acquisition of personal information that threatens user privacy. Game-network providers also forward this data to others, in the following ways: First, depending on the game, a network provider forwards the user requests to the provider hosting the game servers (game-server provider). Second,

several games embed in-game advertisement: Advertisers place real ads on the virtual advertising panels, e.g., for perimeter advertising in sports games. Advertisers then pay for their ads based on complex payout functions [3]. Third, individuals can exchange information between their social-network profiles and their game-network profiles. For instance, people can automatically upload their levels achieved in a game or their trophies won.

So far, while others have studied the privacy practices of SNS [4], this is not the case for game networks. Game networks are different from SN, in various ways: There are several parties responsible for the service provision, e.g., for authentication, playing, purchasing for a game, and these parties are tightly interwoven. Further, the parties responsible for the service provision vary for nearly every game available, and they differ in design, technology, utilization, and intent. Thus, results from SNS do not readily carry over to game networks.

In this work, we study privacy issues in game networks. In particular, we ask 'Is it feasible for a user to understand which party has which personal data?' (Q1). In other words, we analyze if privacy practices are transparent. With respect to the tight connection of game networks and SNS we ask 'Are there privacy threats arising from the connection of game-network providers and SNS?' (Q2). Finally, 'What might help to improve the privacy of the user?' (Q3). To answer the questions, we compare the privacy policies of game-network providers to the requirements stemming from data-protection law. The game networks we consider are the Playstation-Network (PSN), Xbox-Live (XBL) and Wii-Internet-Services (WIS), the three most popular networks by far. The legislative body relevant for our evaluation is the German data-protection law. As the EU is currently harmonizing data protection among its member states, our results are relevant beyond Germany. We evaluate which information the game-network providers acquire according to their privacy policies, whom they forward the information to, and if they inform the user about data usage according to data-protection law – the most powerful mechanism users have in the EU to control the flow of their personal information. In the name of real players we ask the providers which data they have stored and forwarded and evaluate their responses. The study has taken place between February and August 2010.

The impact of our work is high: The privacy practices of game-network providers have not yet been analyzed sufficiently. This is crucial as there are millions of gamers affected, and the information processed may be sensitive.

Paper structure: Section 2 contains some background information and explains the legal situation. We also report on related work. Section 3 describes our study setup, Section 4 gives our evaluation results. We propose measures to protect user privacy in Section 5. Section 6 concludes.

## 2 Background

In this section we give background information on game consoles and online networks. Then we describe in-game advertisement. Finally, we briefly discuss the statutory framework on data protection relevant for game consoles.

## 2.1 Parties Providing Online Gaming

While games with the first generations of consoles have been purely local, today's consoles all feature online gaming. This requires user management, payment mechanisms, hosting of the games, matching similar users for online sessions (matchmaking) etc. In this section we describe the parties involved in online games. These are the game-network provider, the game-server provider, ad servers and third-party providers.

*Game-network provider.* The game network is the gateway to any online access via a console. The network management handles the authentication and authorization of users and offers relevant services. For instance, it provides updates, manages groups of friends, sells updates, games, add-ons etc. Microsoft calls its network 'Xbox-Live' (XBL), Sony 'Playstation Network' (PSN) and Nintendo 'Wii Internet Services' (WIS). At all networks, users have to register before they can access it. PSN and XBL offer one network for all services. WIS distinguishes between Nintendo Club and the Nintendo Shop and states in the privacy policy that, without the user consent, information is not consolidated. It is important that not participating in the network as a player is unrealistic: The providers offer relevant patches, updates and extensions online, i.e., over their networks. Patches are available several times a month, some required for the games and some for the console itself. Downloading these patches, storing them on a disk and installing them manually, as is technically feasible, would not be practical.

*Game-server provider.* Game-server providers host the games. They mediate between players, i.e., create game sessions and assign users to them, etc. Games can be hosted by the game-network providers or by independent companies, e.g., the *game publisher*. For instance, Activision, the publisher of 'Call of Duty', also provides the servers hosting the game. In the case of independent companies, the game-network providers automatically forward (personal) information to the game publishers. The connection between the game server and the game network is often hidden from the user. In other words, a user does not need to know which company in which country operates the game server. This is good from a usability perspective, however, it is difficult with respect to data-protection law.

*Ad-servers provider.* Ad servers serve ads shown in games. We will describe in-game advertisement in Section 2.2. Both game-network providers and game-server providers can connect to ad servers and display ads.

*Third-party provider.* The console and game-network providers have recently started (November 2009) to integrate third-party services. These include Twitter, a music-recommendation service, and Facebook. This might raise new privacy threats: The data available to game-network providers and game-server providers (game publishers) allows them to build comprehensive user profiles. For SNS, this is well known [4]. The connection between both allows game-network providers and game publishers to learn details on their players from the SNS, e.g., habits, friends, interests. The SNS in turn can learn how often a user plays which game,

at which time. The SNS can see this by trophies uploaded, game statistics etc. Thus, not only the trophies can threaten privacy, but also metadata like the upload timestamp. Further, companies providing ads for both game networks and SNS might learn from this as well, e.g., by linking IP information they obtain from the game-network provider for billing purposes.

XBL offers access to all these third-party services, e.g., users can upload images like game screenshot [5] and can browse Facebook photos. PSN users can send game statistics and information on items shopped to Facebook [2], upload videos to Youtube, and browse photos at Facebook and Picasa<sup>1,2</sup>. WIS does not offer such a third-party integration.

## 2.2 In-Game Advertisement

Several games feature in-game advertisement (IGA). A unique selling point of IGA is that players accept it as making games more realistic [6]. We distinguish two variants of IGA: Static and dynamic in-game advertisement. The first variant is hard-coded, i.e., part of the game, and can be refreshed with software updates. With the dynamic variant in turn, ads are loaded from ad networks on-the-fly. Advertisers then pay based on complex payout functions. Both the Sony and Microsoft console feature dynamic advertisement. Sony has integrated the IGA Worldwide and Double Fusion in-game advertising networks. Microsoft uses the network of its subsidiary Massive Inc. and 18 further providers<sup>3</sup>. The effectiveness of IGA depends on how good the ad-placement algorithm predicts the interests of the users. This in turn brings ad-network providers to learn as much as possible about their customers, i.e., to collect sensitive personal information.

## 2.3 Legal Background

Since the EU Directive 95/46/EC has been issued, all EU member states have established data-protection regulations for services on the Internet. Many countries try to define regulations independent from the technology they apply to. Thus, first we have to find out which law is the relevant one for the parties involved in offering online services for consoles. This includes the relevant country and the law within the country.

With respect to [7], game networks are subject to the German Telemedia Act (Telemediengesetz, TMG). This law is relevant for services on the Internet if the service is a Telemedia service in terms of §1 p. 1 s. 1 TMG. It applies to all electronic services of information or communication except for telecommunication services (§3 No. 24, German Telecommunication Act, TKG), telecommunication supported services after §3 No. 25 TKG and broadcasting services (§2 German

<sup>1</sup> [http://de.playstation.com/ps3/support/system-software/detail/item289447/Update-Features-\(Ver-3-40\)/](http://de.playstation.com/ps3/support/system-software/detail/item289447/Update-Features-(Ver-3-40)/)

<sup>2</sup> <http://blog.us.playstation.com/2010/06/28/playstation-3-system-software-update-v3-40-available-soon-2/>

<sup>3</sup> <http://privacy.microsoft.com/de-de/fullnotice.mspx>

Broadcast Services State Treaty, RStV). The game-network providers and the game-server providers do not fall under these exceptions, so the TMG is relevant.

The scope of the TMG for international data processing depends on the home-state regulation in §3 p. 1 TMG. It says that (1) the German law is the relevant one if the provider is located in Germany. However, it further says that (2) if the provider is outside of Germany but within the EU, the law of the country from which the provider offers the service is the relevant one (§3 p. 3 TMG, §1 p. 5 Federal Data Protection Act, BDSG). For XBL and WIS (1) holds as they are located in Germany. For PSN however and according to (2), the British privacy law has to be applied because their domicile is not Germany but the UK.

With the TMG and the BDSG being the relevant legislative body and according to 95/46/EC, a provider has to fulfill several requirements. We will investigate to which extent providers act according to them. 95/46/EC harmonizes data protection within the EU, i.e., in this work we refer to German law (also in the PSN case) but this will hold for EU legislation as well.

## 2.4 Related Work

Game networks have not yet been studied sufficiently with respect to privacy. [7] describes the legal issues relevant for overlay networks, which, by subsumption, also hold for game networks. [4,8] describe large networks of interconnected users. However, they refer to social networks where users tend to establish the contacts explicitly. The assignment of users to game sessions in contrast takes place automatically, based on player characteristics. Others, e.g. [9], analyze in-game advertisement, but leave data protection aside. [10,11] investigate website advertisement and investigate privacy threats related. This as well cannot easily be mapped to game networks: Game networks use complex payout functions requiring a lot of personal information, much more than website advertisement.

## 3 Study Procedure

In this section we describe the two steps of our evaluation: first, the analysis of the privacy policies and, second, the request for information. Further, we describe differences between the game-network providers we have investigated.

*Privacy-Policy Analysis.* An important design decision of this study is to analyze the privacy policies of the providers (and nothing else) to learn about the privacy practices of providers. This is to avoid relying on insider knowledge regarding the data processing at the providers and to keep our study objective. Further, law requires providers to inform users of data collection and processing in advance. Thus, users assess providers by characteristics accessible from an external perspective, i.e., the privacy policy, and we do so as well. In more concrete terms, we analyze the privacy policies and the general terms of usage. Some providers have more than one privacy policy, e.g., a general and a specific one, as they call them. We consider all of these policies. We evaluate the providers

according to the following criteria: the availability of a privacy policy, the law they deem relevant, information on data collection and forwarding, information on automated data processing like cookies, the way they integrate in-game advertisement, information on the right to opt-out, giving and revoking consent, and the availability of a contact address.

*Non-Transparency vs. Violation.* With any assessment of the provider we will state whether the practice of the provider fits our interpretation of the law. In several cases the practice might be, but is not necessarily a violation of the law. We would need further details, or it would require a court (of ultimate resort) decision to decide if this was a violation. In any case, it is not transparent for the user what the provider does with the data. In the assessment we will use the words ‘non-transparency’ and ‘violation’, denoting them with ▲ and ♯ respectively.

*Request for Information.* An individual has the right to request from a provider which personal information it has stored about him. The provider has to reply immediately, i.e., within two weeks realistically [12]. This arguably is one of the most important mechanisms to track one’s personal information. To test its effectiveness, we ask PSN, XBL and WIS for personal information on behalf of real players. We also do this with several game publishers. We have sent our requests via postal letters, and we have identified ourselves (the requester) with our MAC and IP address, the serial number of the device and the user-account name. We have requested any information that the provider stores *about* the requester, the *attribute names* and *attribute values*, and the *purpose of the acquisition* of the data. Further, we have requested *which data* has been forwarded, to *whom* and for which *purpose*. We have considered any response received until now.

A common approach to substantiate results would be to repeat the experiment, i.e., send several requests. In our case however, the providers might see what our intention is and behave differently, compared to ‘normal’ requests. To observe realistic behavior, we have contacted a provider at most two times.

*Game-Network Providers.* We analyze the three game-network providers PSN, XBL and WIS. The WIS privacy policy has a distinctive characteristic: It claims that no information WIS acquires can be linked to an individual, as long as the Wii-shopping-channel account is not connected to the Club-Nintendo account. A user can connect both in his personal settings. So WIS acquires data but states to be unable to identify individuals by it. To better compare the three game-network providers, we will investigate the case of connected WIS accounts if not stated differently.

## 4 Evaluation

We now evaluate the privacy practices of the game-network providers. We then focus on privacy threats that might result from connecting SNS and game networks (Section 4.2). Last, we investigate how PSN, XBL and WIS deal with the right of individuals to access their personal data (Section 4.3).

## 4.1 Privacy Policy

We now report on our evaluation of the privacy policies of game-network providers according to the criteria from Section 3. For citations we use another font.

**Table 1.** Overview privacy-policy analysis

Assessment criteria	PSN	XBL	Wii
Relevant law			
Privacy policy available	▲		▲
Data acqu. (kind of data)	▲	▲	
Data acqu. (scope of data)	↯	↯	
Data acqu. (purpose)		▲	
Data acqu. (usage data)	↯		
Data forwarding		▲	
Automated processing	↯	▲	↯
In-game advertisement		▲	
Giving & revoking consent	↯	▲	↯
Contact address		▲	

**Table 2.** Usage-data attributes

Attribute	PSN	XBL	Wii
IP address	✓	✓	✓
MAC address	✓		
console id	✓	✓	
user id	✓	✓	✓
settings	✓		✓
time/date of usage	✓	✓	✓
games played	✓	✓	✓
chat usage	✓		
content accessed	✓		✓
game statistics	✓	✓	
friend list	✓		
products purchased	✓		✓
credit card inform.	✓		

**Relevant Law.** The relevant law is the TMG. *XBL* does not state anything about the relevant law, *WIS* says that the contract the user agrees to when registering is subject to German law. Both is acceptable, as no information on the relevant law is required, but if it exists, it has to be correct. *PSN* in contrast says in their general terms that, to the extent permitted by law, they will handle all claims by the law of England. According to Section 2.3, this is valid.

**Availability of privacy policy.** §13 p.1 s.3 TMG: *Each customer must be able to obtain the privacy policy easily and at any time.*

Though all network providers do have privacy policies, users already encounter several difficulties when they simply want to see them. The *PSN* privacy policy can be found easily. In the policy itself *PSN* refers to a page where the most current version is available. However, it points to a dead URL<sup>4</sup>. For *XBL*, users can find a link to the privacy policy. It consists of a **general** policy, valid for all Microsoft services, a **compressed** version and a **special** one for individual services, e.g., for *XBL*. For *WIS*, due to the separation of the game network and the shop, finding the privacy policy is difficult. It exists stand alone for the *Wii-Shop-Channel* and as a part of the general terms for the game network. However, the section in the general terms is marked with the wrong caption. Further, when selecting the German language and then opening the policy, it is different from the one shown when Nintendo picks a language automatically.

We classify the *PSN* practice and the *WIS* practice as non-transparent.

<sup>4</sup> <http://network.eu.playstation.com/legal>

**Information on data acquisition.** §13 p.1 s.1 TMG: *A provider has to inform on (i) the kind of data, (ii) the scope and (iii) the purpose of data acquisition and usage. The purpose specification can be omitted when obvious.*

*Kind of data.* The legislator requires the providers to state attribute names or meaningful categories, e.g., shipping address, of data which they collect for the registration. *PSN* names attributes, e.g., name and e-mail address, and meaningful categories, e.g., postal address. However, they also refer to attributes like . . . . Thus, it is not clear if the list is complete, i.e., we see a non-transparency. *XBL* states attribute names and meaningful categories as well. However, they list the attributes acquired in the general privacy policy, which covers access to websites as well as Microsoft services for mobile phones etc. Thus, since it is not clear which attributes *XBL* collects, this is a non-transparency as well. The *WIS* policy names the attributes necessary for a registration.

*Scope of data (storage time).* In the *PSN* privacy policy we do not find a hint on how long data is stored or on how to delete it. This is a violation. *XBL* gives no information on how long the data is stored either, i.e., this is a violation as well. *WIS* provides an email address which a user can contact to delete the data.

*Purpose.* *PSN* states explicitly which purpose they acquire personal data for, e.g., for network gaming, community functions etc. *XBL* states several purposes, ranging from providing the requested service to advertisement. Again, as Microsoft states the purpose in the general policy, it is unclear if this holds for the *XBL* game network as well. We classify this as non-transparent. *WIS* clearly states the purposes access to websites, registration for a newsletter and email subscription.

*Information on the acquisition of usage data.* Besides the data providers acquire when registering at the service (inventory data), providers also acquire data when individuals use the service (usage data). All providers list the attributes of the usage data collected. This includes the IP address, the usage behavior etc. (see Table 2). *PSN* states that, to enforce the general terms of use, they may store any information on chat and speech data, without informing the user beforehand. This is a violation. They do so without any well-founded suspicion and, as this clause is 'surprising', it also violates the German Civil Code.

**Forwarding of data.** §13 p. 1 s. 1 TMG: *Each provider has to state which personal data is forwarded to others.*

*PSN* states three kinds of receivers of personal information. The first ones are companies providing the *PSN* service. *PSN* states that the receivers have to act according to the *PSN* privacy policy, and that *PSN* regards herself responsible for the data. Second, other subsidiaries of Sony Computer Entertainment have access to the data. In this case, *PSN* does not state the purpose of data forwarding. As *PSN* is a worldwide service, data is forwarded to countries outside the European Economic Area, i.e., countries with different data-protection

laws. PSN informs on this. Third, PSN also forwards personal data to game communities, third-party publishers and social network sites at the time when a user accesses it. Here, it is important that the PSN states that the receiver of the data is responsible for the personal data, i.e., another policy takes effect. *XBL* states to forward data to other countries as well. According to their privacy policy, personal data can be stored and processed in any country where Microsoft has a related company or a branch, or where their service providers have offices. Microsoft states to act according to the Safe-Harbor Agreement. It establishes that the data transfer to the US complies with the EU directive 95/46/EC. Normally, this agreement is relevant for EU subsidiaries of Microsoft only. But from the Microsoft privacy policy, a user gains the impression that this holds for companies outside of the EU and the US as well. We deem this non-transparent. *WIS* states that they do not sell personal information and use it only for its own purposes and the ones of their subsidiaries.

*Summary.* All providers are international and have subsidiaries they forward personal data to. A user is not able to find out which companies belong to a provider. Thus, the data flow is non-transparent. However, since relationships of companies are likely to change over time, it is adequate to name the receivers of the data in forms of categories. It then depends on how the providers handle requests for information (Section 4.3) whether this is a violation.

**Information on automated data processing.** §13 p.1 s.1, s.2 TMG: *Each provider has to inform about the automated processing of personal data if the processes give way to the identification of an individual. In particular, the obligation to inform includes (i) the kind of data, (ii) the storage period (scope) and (iii) the purpose of processing.*

*PSN* uses cookies to acquire specific information about the users, to track the access and usage of PSN, to deliver the service and to store the relevant language. The formulation specific is vague. Further, there is no information on the storage time, i.e., if session or persistent cookies are used, for how long, or on how to remove them. This is a violation. *XBL* uses cookies for the login to specific services, for the personalization of the service and to place adequate advertisement. *XBL* states to use session cookies, which will be removed when logging out or closing the browser, and persistent cookies. *XBL* explains how to remove cookies. We deem this sufficient to meet the storage-time requirement. Further, Microsoft states which information is stored in the cookies. Thus, Microsoft informs on the kind, purpose and scope of cookie usage. Microsoft uses also Webbeacons, i.e., content like transparent one-pixel images users download (unknowingly) and providers then track. Microsoft uses this for statistical purposes, for cobranding services and advertisement. Further, under certain circumstances, Microsoft uses Webbeacons of third parties that build statistics. *XBL* says that no such Webbeacons are allowed on Microsoft websites that give way to the collection of personal data. On the other hand, *XBL* states that they build aggregated statistics. This is comparable to web-statistics tools which violate data-protection law in Germany [13]. Here, further details are required to

decide if this is a violation. However, formulations like specific services or under certain circumstances are non-transparent. *Wii* states to use cookies to collect information on the websites a user visits and the products he is interested in. Further, *Wii* states to use cookies to check if a user is already registered, and permanent cookies to store the preferred language of the user. Webbeacons are also used, e.g., to track users. *Wii* does not say how long cookies are stored, i.e., violates the law. The purpose *Wii* states is to provide content interesting for the user and for marketing purposes.

**In-Game Advertisement.** *PSN* states to create personalized profiles to predict the user intent and interests. To do so, *PSN* states to store the IP address, the MAC address, the position in the game where the ad is placed, how long the ad has been visible, its size and the perspective the user has seen it from. This information is not only stored by *PSN*, but *PSN* also forwards it to companies that place the ads. However, it becomes clear to the user what kind of information *PSN* processes and forwards. *XBL* does not explicitly use the term in-game advertisement. They state that many services offered by Microsoft partners are supported by advertisement. Due to the very general overall privacy policy it is difficult to understand if Microsoft as the game-server provider uses in-game advertisement. We classify this as non-transparent. The *WIS* privacy policy does not mention in-game advertisement or personalized ads.

**Opt-Out.** §15 p.3 TMG: *If the provider informs the user on his right to opt-out, the provider is allowed to build usage profiles for the purpose of advertisement, market research, and to adjust the service to market needs.*

Regarding this point, all providers behave in line with law. *PSN* creates pseudonymous profiles. However, they inform the user on his right to opt-out from receiving marketing information. They refer to the account-setting page, where the user can disable this. *XBL* creates pseudonymous and personalized profiles. They also refer to a page where the user can deactivate personalized advertisement. Users can do so for the device they currently use or for their entire account, i.e., their Live-ID. This allows to deactivate personal and pseudonymous profiles. *WIS* creates pseudonymous profiles as well and explains how to opt-out.

**Giving and revoking consent** §12 p.1, §13 p.2 TMG: *Acquisition and usage of personal data are allowed only if permitted by law, or if the user consents. It must become clear which purpose the user consents to, and which practice is already legitimated by (any) law. Further, the user has to be aware of the fact that he is consenting. The user must be informed that he can revoke his consent at any time.*

In particular, requesting the consent of the user is required when building personalized profiles, acquiring more data than necessary to provide the service and when forwarding personal information to non EU countries. All providers request user consent to their privacy practices.

*PSN* creates personalized profiles, acquires more data than necessary to provide a service, e.g., the postal address, and forwards data. Thus, giving consent

is required. PSN also requests the consent for using cookies. It does not become clear which purpose that requires a consent they use cookies for. The PSN privacy policy states that using their service after a modification of the privacy policy is equivalent to giving consent consciously. The same holds for the forwarding of personal information. This is a violation of the law. Further, PSN does not inform the user that he can revoke his consent. This is another violation. According to its privacy policy, *XBL* creates personalized profiles, forwards data to companies not necessary to offer the service, and collects data not necessary to this end. Thus, user consent is required. However, a user cannot see in detail from their privacy policy which practices actually do require consent. We classify this as non-transparent. As mentioned before, *XBL* offers an interface to revoke the consent for advertisement. Further, they inform the users that they can revoke the consent. This is in line with the law. *WIS* explicitly states in a paragraph purposes which they request consent for. This is transparent. However, a closer look shows that this paragraph also includes practices that do not require user consent. For instance, this is the case when the provider uses personal information to improve a website. Again, a user cannot see what exactly the consent is required for, and what is legitimated by law anyhow. As we have explained, *Wii* distinguishes between two kinds of accounts, one for playing and one for the shop. They state that by connecting both accounts a user automatically consents to building a personalized profile. However, this implicit kind of giving consent is a violation. In line with law, *Wii* points out that the user may revoke his consent.

*Summary.* All providers request user consent, as required by law, considering their purposes. However, they do not make clear what is already legitimated by law, and which practices require consent. Further, giving consent must be consciously, but this is not always the case.

**Contact Address** §15 p.1 no. 1, no. 2 TMG: *Providers have to provide a contact information.*

The *PSN* and *WIS* privacy policies contain concrete contact addresses. *XBL* states how to contact a person responsible for data protection, a phone number, a web form and a postal address. When using the web form however, one has to consent to the privacy policy before being able to ask questions regarding the policy itself. Further, the privacy policy referenced in the form cannot be correctly displayed with Firefox. Last, the contact form the policy displayed refers to is different from the one we came from. Overall, we deem this non-transparent.

## 4.2 Interconnection of Console Networks and Social Network Sites

The connection of game networks and SNS since 2009 are likely to raise new privacy threats. We analyze how the game-network providers address this issue in their privacy policy. *PSN* states that data can be forwarded to, say, SNS if one

accesses such a service via one’s PSN account. The purpose of the data forwarding, according to PSN, is to provide the services and related research and analysis. We do not know what research and analysis include and classify this as non-transparent. PSN states that, when forwarding data to a SNS (here Facebook), the privacy policy of the receiver is the relevant one. *XBL* does not explicitly use the terms ‘social network site’ or ‘Facebook’, but states to use cobranding and to offer some services referred to as alliance with other companies. We assume that, here as well, the privacy policy of the receiver is the relevant one. This conforms to law if XBL informs the user when data is transferred.

### 4.3 Request for Information

§13 p.7 TMG, §34 BDSG: *Each customer can ask a provider to inform her on her personal data. The provider has to list all data stored and forwarded.*

**Table 3.** Responses to the request for information

	PSN	Activision Electronic Arts Epic Games Ubisoft	Rockstar Games	XBL	Activision Electronic Arts Ubisoft	WIS	Hudson Entert.
Response time	1m, 14d	↗ ↗ ↗ ✓	14d	↗ ↗ ↗	20d	20d, 1m, 1m	↗
Data acquisition	-, ✓	↗ ↗ ↗ ✓	↗	↗ ↗ ↗	✓	-, -,	↗
Data forwarding	-, ↗	↗ ↗ ↗ ✓	↗	↗ ↗ ↗	✓	-, -,	↗
No Complaints	-, ▲	↗ ↗ ↗ ✓	✓	↗ ↗ ↗	✓	-, -,	↗

Our evaluation covers all assessment criteria relevant according to law, as well as general information on the interaction with the provider. It states whom we obtained a response from, within which time window, if the provider has replied with the data acquired and stored, the data forwarded, the purpose of any data forwarding, the receiver, and if the request has been answered without complaints. Table 3 gives an overview. Multiple entries for the same provider means that we have had repeated interactions. For each player we will first describe our experiences with the game-network providers, the ones with the game publishers follow. Complementary information can be found on our web site<sup>5</sup>.

We have approached the game-network providers and game-server providers in the name of three real players. In the name of a PS3 user we have asked PSN, Activision, Electronic Arts, Epic Games, Rockstargames and Ubisoft. For the Xbox user we have requested information from XBL, Activision, Electronic Arts, and Ubisoft, for the Wii users WIS and Hudson Entertainment.

**PSN.** We have sent 6 requests for information in the name of the PSN user.

<sup>5</sup> <http://privacy.ipd.kit.edu>

*Game-Network Provider.* PSN has answered our request after one month by requesting a copy of the passport and asking if they could limit the information sent to one year; we did agree. 14 days later we have received a detailed list of data acquired, stored and processed, together with a description on how to read the table, explanations of the database schema etc. This includes 15 inventory attributes (see Table 4).

**Table 4.** Inventory-data PSN

Attributes 1	Attributes 2
Identifier	Last Deposit Amount
PSN Account ID	Last Deposit Date
Login Name	Account Update
Pseudonym	Reg. Console ID
Account Status	Gender
Address 1 – 3	Day Of Birth
City	Language
Zip Code	Account Creation
Province Code	Opt-In Direct
Country	Opt-In-3rd-Party
Country Currency	EULA-Version
Wallet Balance	

**Table 5.** Events PSN

Events 1	Events 2
Authentication	Verify (Payment)
Authorization	Activate Console
Authorize DRM	View Product
Create Account	Add to Cart
Change Payment Infor	View Category
Change Opt-In	Purchase Product
Credit Card Auth.	Download Content
Credit Card Charge	Redownload Store
Purchase	Purchase Info
Deposit - Charge	Create Session
Lookup Voucher	Delete Session

Besides the inventory data, PSN acquires two kinds of usage data: They call the first one **transactions**, the second one includes connection information to the network etc. Transactions refer to any action related to the Playstation store. For each transaction they store 57 attributes, including the name of the buyer, his day of birth, the product etc. Further, PSN has sent us an overview of the transactions, which we refer to in the following. Transactions, as far as we can see from the answer, refers to **downloads**, **product sale**, **voucher redemption**, and **revenue realization**. Product sale also includes access to demos of games etc. For any transaction, they store the transaction type, a time stamp, the identifier and pseudonym, the quantity, price, currency, the medium used to buy the product (e.g., PS3, PSP), the product name and a product category.

The second kind of usage data comprises 22 event types (see Table 5). The events have between 4 and 10 attributes, e.g., specifying the account ID, IP address, console ID, name of the credit-card owner etc. As one can see, the data PSN stores is not free of overlap. However, we present it here as given by the PSN response. For our PS3 user, PSN has reported 1760 events stored. This allows to build a comprehensive user profile.

Next, we look at the forwarding practices. PSN has stated in their response that, for purposes given in the privacy policy, data is forwarded to Sony-Computer-Entertainment companies and to external service providers. This is a violation, as this category is too unspecific.

Further, PSN states we cannot guarantee that the data provided is correct and complete. This is insufficient from a legal perspective.

Summing up, PSN has answered our request at the level of detail required by law, in a human readable way. Further, the attributes fit the ones in their privacy policy (cf. Table 2). However, they have not correctly informed us whom they have forwarded our data to, and state that the response might be incomplete.

*Game Publisher.* From the game publishers, only Ubisoft has answered, stating that they do not store any personal information and referring us to PSN. From all others we did not get any response. This violates the law.

**XBL.** We have sent 4 requests for information in the name of the Xbox user to XBL, to two different addresses, one in Germany, one in the USA. XBL has answered neither one. From the game publishers, again, Ubisoft has answered our request. They claim to not store any personal data. Activision did not respond. EA games gives a dead contact address in their privacy policy. We have sent a second request to another address but have not obtained any response. Summing up, except for Ubisoft, the providers violate the law.

**WIS.** We have sent 2 requests for information in the name of the Wii user.

*Game-Network Provider.* WIS has replied to our request after 20 days, requesting the serial number of our Wii and a copy of the sales slip. One month later, we have received a response that, to answer our request, the MAC address and IP address have to be correlated with our name. They have asked if we agree to this procedure. In their final response, WIS states that they deem the data-protection law not relevant for them, as they perceive the data they store as anonymous. They further say that, in fact, the personalization of the data stored had become possible with the name from our request. However, as they have stored credit card and purchasing information, they obviously have the possibility to correlate the usage data with individuals. Thus, the information stored is at least pseudonymous, i.e., one has the right to request that information. We do not classify this as a violation as WIS has answered our request.

WIS stores three kinds of information: **basic information**, **shop-channel data**, and two **network-communication logs**. See Table 6. Further, they explicitly state which data is stored and processed in which country by which company. Countries they name are Japan and the US.

**Table 6.** WIS data

basic data	shop data	network communic.
Wii number	purchasing points	game title
serial no	purchasing game	user nickname
device region	balance	login time
country	time / data	current IP
register date	name of game	time of msg.
Wifi MAC	current IP	
Bluetooth MAC		

The WIS response fulfills the requirements from law. However, in their second response WIS states that they will provide only such information where doing so is reasonable at a technical level. This is a violation.

*Game-Publisher.* We have sent a request for information to Hudson Entertainment. However, we got back the letter with the information that the forward time expired for the address used – the address we took from the privacy policy. We have sent another request to a different address, but did not receive any response. This is a violation.

Summing up, the request for information fails in practice. From 12 requests we have sent, providers have answered only 4, and some replies are incomplete. Further, with up to three months to come to results, users cannot effectively track their personal data.

#### 4.4 Summary

Our evaluation shows that the means to track the flow of one's personal information are insufficient (Q1, Q2). This is due to often vague statements on which information is acquired, stored or processed, and to unspecific formulations regarding the potential receivers in case of data forwarding. The request for information, the most powerful means of a user to track her personal information, yields results that are particularly unsatisfactory.

## 5 Proposals

In this section we will answer Q3 (What might help to improve the privacy of the user?). We only focus on what we have not already deemed non-transparent or a violation. We derive our proposals from the evaluation just presented.

- P1. The forwarding of personal information from the game-network provider or the game publisher to ad servers puts user privacy at risk. Actually, such information is transferred to prove when, where and for how long the ad impressions have been shown. Put differently, millions of users have to trust the game-network providers, game publishers and advertisers. A potential solution might be billing models where personal information is not transferred, or only in case of a breach of the agreement.
- P2. Serving a privacy policy common for all services and specific ones for the individual services sounds wise, at least at first sight. However, we have observed that providers overload the common policy, like collecting any practice conceivable, so that the real practices become non-transparent. We propose that there should be individual policies for any service, or the common policy should only cover the practices common to all services addressed.
- P3. Today's highly complex consoles require maintenance, i.e., software updates. We do not see any reason why a user has to be registered at the game network to download updates and fixes. We propose, in the style of the WIS distinction between shop and gaming data, a separation of entertainment, shop and maintenance services provided.

## 6 Conclusions

Game consoles and the corresponding online networks currently offer a variety of different services. To provide these services, game-network providers collect and process personal information. For advertisement, they also forward the information to third parties. This puts user privacy at risk.

In this paper we have analyzed the privacy policies of Sony Playstation, Microsoft Xbox-Live and Nintendo Wii, and have compared them to their actual data-processing practices, as far as they are observable from an outside perspective. Our results are that in many cases the provider practices are non-transparent or even violate law. In particular, most providers which we have sent a request for information to did not send any or only an incomplete answer. Given these insights, we have compiled a list of proposals that might help to make the practices more transparent and to protect user privacy.

## References

1. Spiegel. Playstation 3 im Test – Das sexy Paradox (March 2007), <http://www.spiegel.de/netzwelt/spielzeug/0,1518,473311,00.html>
2. Sony Computer Entertainment America Inc. (SCEA). To offer richer online social experience to playstation®3 computer entertainment system owners with facebook integration (2009), [http://www.scei.co.jp/corporate/release/091118\\_e.html](http://www.scei.co.jp/corporate/release/091118_e.html)
3. Interactive Advertising Bureau. In-Game Advertising Measurement Guidelines (2009), [http://www.iab.net/iab\\_products\\_and\\_industry\\_services/508676/guidelines/in-game](http://www.iab.net/iab_products_and_industry_services/508676/guidelines/in-game)
4. Gross, R., Acquisti, A.: Information Revelation and Privacy in Online Social Networks. In: WPES (2005)
5. Microsoft Press Pass. Xbox unveils entertainment experiences that put everyone center stage (2009), <http://www.microsoft.com/Presspass/press/2009/jun09/06-01E3PR.mspx>
6. IGA Worldwide: Landmark IGA-Nielsen Study: 82% of Consumers React Positively to Receiving Contextual In-Game Ads During Game Play (June 2008), <http://www.igaworldwide.com/aboutus/pr/pressreleases/landmark-iga-nielsen-study.cfm>
7. Raabe, O., Dinger, J.: Telemedienrechtliche informationspflichten in p2p-overlay-netzen und bei web-services. Computer und Recht (2007)
8. Zhou, B., Pei, J.: Preserving privacy in social networks against neighborhood attacks. In: ICDE (2008)
9. Yang, M., et al.: The effectiveness of ‘in-game’ advertising: Comparing college students? explicit and implicit memory for brand names. Journal of Advertising (2006)
10. Yan, J., et al.: How much can behavioral targeting help online advertising? In: WWW. ACM, New York (2009)
11. Haddadi, H., Guha, S., Francis, P.: Not all adware is badware: Towards privacy-aware advertising. In: Godart, C., Gronau, N., Sharma, S., Canals, G. (eds.) I3E 2009. IFIP Advances in Information and Communication Technology, vol. 305, pp. 161–172. Springer, Heidelberg (2009)
12. Bundesdatenschutzgesetz: Bdsg; kommentar (2010)
13. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. Datenschutzrechtliche Bewertung des Einsatzes von Google Analytics. ULD (2009)