The Collection and Use of Player Information and Gameplay Data from Online Video Games

The 1984 movie *The Last Starfighter* portrayed a boy plucked from obscurity to serve as an ace pilot in an intergalactic war. The mechanism used to identify and recruit the boy was, at the time, a novel one: a video game.

While *The Last Starfighter* was indisputably science fiction at the time it was released, the use of a video game for such recruiting purposes (aliens aside) no longer seems so far-fetched. Indeed, the increasing realism of video games, combined with their increasing online connectivity, makes games powerful tools for targeted marketing, laboratories in which to test real world hypotheses, and even talent pools for all types of recruiters.

An Overview of Online Video Games

There are three main types of video games that are played online: (i) web-based games, (ii) computer or console-based games with online connectivity, and (iii) massively multiplayer online games. Web-based games are those that run through a standard web browser and often require little or no software be downloaded onto a computer. These games run the gamut from relatively simple in design (e.g., MSN Games with its puzzles, trivia and poker) to extremely complex (e.g., Second Life, which allows its users to create residents in a virtual online world).

Games with online connectivity are typically stand-alone computer or console-based games that require the player first to purchase the software at a retail store like Best Buy or GameStop. These can be played in either single or, via the internet, multiplayer modes. An example is Civilization IV, an empire-building game that, once purchased and installed, allows the user to play alone opposite one or more computer-generated opponents or, by connecting through an internet portal or local area network, against up to eight real life opponents.

Finally, there are massively multiplayer online games. These games, sometimes called MMO games, generally also require the player to purchase the software and install it on the player’s computer. Unlike games that merely have online connectivity, however, these games are designed to be played exclusively online with other people (often with thousands of players concurrently operating in a single online world). World of Warcraft, a fantasy-based MMO game with 6.5 million registered users, each of whom

"Gamer and gameplay data can be fantastically valuable when collected properly and used in ways that are legally authorized. Maximizing this value, however, requires developers to consider early in the game development design process ways they might want to commercialize the data."
can create and “navigate” characters through the virtual world of Azeroth, is a widely known example.

Make Data, Not War

Online games, whatever their nature, generate an enormous amount of data. Operators of online games collect data from initial online registrations and subsequent transactions, such as the player’s name, email address, and possibly street address, age and other demographic information. Operators also collect a stream of data generated from each player’s gameplay, such as how long the player is logged on, how frequently the player logs on, what levels the player achieves, where within the game the player travels, and other information that reflects how a player behaves within the game. Both player and gameplay data can be used for marketing purposes related to the game itself or for products or services that the game’s operator thinks might interest to players.

The volume of behavioral data revealed by online gameplay is massive. Nonetheless, computer servers can and do affordably capture and keep such data on an individual and aggregate basis. It is this data, combined with the identifying information entered by the player, that is potentially of the greatest value to online video game operators and third parties. For instance, an operator can use the data to help the game’s developer design ways to improve the individual player’s experience, such as making particular objectives easier or harder to achieve depending on how much skill the player exhibits through gameplay play. An advertiser can use the data to measure how many times a player passes by, or for that matter, stops on, the advertiser’s in-game product placement, and what types of players appear to be attracted to the ad.

This data also creates the most legal uncertainties. What kind of personal traits can be extrapolated from the data and how can such extrapolations be used? How widely can the data itself be shared? The US Army already uses video games to recruit and even train soldiers. Could the operator of an online game which simulates wartime combat share with Army recruiters the contact information and profiles for its highest level players? Some companies use online games to train managers to build teams, map out strategies for achieving shared objectives and the like. Could game operators disclose to professional recruiters the demographic profiles or even individual identifying information of players who accumulate the greatest in-game wealth or build and lead teams successfully?

Tracking gamers’ movements for commercial purposes raises serious privacy concerns. Although bills have been introduced in Congress, there is currently no single federal law that regulates the collection of consumer information over the internet. Instead, a collection of laws and judicial decisions define privacy law in this area – and their applicability in the online video game context remains relatively untested. The Electronic Communications Privacy Act of 1986 has been interpreted so narrowly that it has virtually no adverse effect on companies’ ability to plant cookies, web bugs and other devices to access personal information and web browsing habits. Section 5 of the Federal Trade Act (Section 5), which outlaws “deceptive and unfair trade practices,” was written decades ago before the internet even existed. And although there are various industry-specific laws written with the internet in mind (e.g., Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act of 1996), these have no direct applicability in the video game industry. Indeed, the only federal law that is directly on point is
the Children’s Online Privacy Protection Act (COPPA) which regulates internet sites aimed at children. COPPA restricts a “website or online service targeted to children” younger than 13 that knowingly collects information from such children from collecting and using personally identifiable information without verifiable parental consent.

Beyond the federal legal landscape, many states require commercial websites and online services that collect “personally identifiable information” about a person to post a privacy policy which informs the person of that fact, for what purposes the information will be used and with whom it will be shared. In certain circumstances, these laws require the person be permitted to “opt out” of some or all of the data collection and/or sharing. Other countries have data privacy schemes of their own; in many cases these differ significantly from those existing (or not existing, as the case may be) in the US. For instance, other country’s laws often contain “opt-in” rather than merely “opt-out” consent requirements before data can be shared with third parties.

In addition, what can be done with player data depends in large part on who owns it. US businesses operate on the assumption that whoever collects customer data – regardless of whether the data constitutes an original work of authorship protected by the copyright laws – owns it. While this has been upheld recently in some US courts, various foreign courts take the exact opposite position.

That said, in the US there do not appear to be any specific legal restrictions on the collection or use of gameplay data. Just as “click stream” data—the record of what websites an internet user visits, how long the user remains on a particular page, what portions of the page the user clicks his or her mouse on or even scrolls over – from e-commerce retail websites is largely unregulated, gameplay data appears to be free from regulation as well. Other countries, however, take different approaches. The laws of other countries are important to online games because these games can fairly easily be accessed from players in other parts of the world, and the laws of a player’s country of residence arguably govern how that player’s data can be collected and used. And here in the US, given the attributes that could make gameplay data so valuable – the length of time over which it is collected and the degree to which the data might be viewed as a proxy for the player’s real world talents or anti-social proclivities – governmental regulation may not be far off. In light of recent allegations that phone companies improperly shared customer phone data with the National Security Agency—allegations the phone companies deny—some might fear the consequences of a government interest in game play data. An ill-thought-out policy on the part of companies that hold gameplay data governing player data could result in a public relations nightmare and would almost surely result in lawsuits.

**Mining Your Own Business**

So, can player data be collected and utilized in a manner that maximizes its value to the operator, third parties and, arguably, the gamer – all without unduly exploiting the gamer and violating his or her privacy rights? End user license agreements (EULAs), terms of service and privacy policies, singly or in combination, attempt to negotiate the regulatory and judicial landscape. However, there are issues with each of these approaches (e.g., when does such an agreement become a contract of adhesion or what if the player is actually a minor), not to mention that, without overarching federal legislation, the legal landscape is constantly shifting (requiring decisions about when and how to update these agreements).
The End Game

For the reasons described, gamer and gameplay data can be fantastically valuable—provided that is collected wisely and used in ways that do not invite legal challenges. Maximizing this value, however, requires developers to consider early in the game development design process ways they might want to commercialize the data. It requires publishers to draft their EULAs, terms of service and privacy policies broadly enough to permit unforeseeable uses. Finally, it requires operators to give careful thought to how, in practice, they collect and store data in order to ensure that the data with more limited permissible uses can be segregated from data with broader permissible uses.

Recommended Cheats

The worldwide reach of the internet presents a special challenge in determining which laws govern privacy issues raised by online games. Moreover, no amount of research and planning will prevent state, federal and foreign governments from changing the rules in the future. Nonetheless, online video game operators who want to take a conservative approach to privacy matters—both to lessen the risk of lawsuits and to preserve the broadest possible rights to use player information and gameplay data in the future—can look to the Federal Trade Commission’s Guidelines for Online Privacy Policies for guidance as to what future regulations might look like. Certain “conservative best practices” for online game operators who wish to maximize the value of games and gameplay data they collect can be gleaned from these guidelines and other legislative initiatives. Such practices include the following:

• ask players to opt-in to data gathering and sharing rather than just opt-out;
• disclose to players what data the operator collects, how the data is collected and what the operator intends to do with it;
• use the best means technologically feasible to verify each player’s age in order to ensure that the permissions granted are not voidable contracts;
• segregate databases according to the EULA, Terms of Service and privacy policy in place when the data was collected;
• segregate databases according to the country from which the data originated;
• adhere to COPPA no matter how adult-oriented the game; and
• test the site and its operation routinely to ensure that actual practices conform to stated policies.
*Ms. Christ is a partner and Mr. Fox is an associate in the Los Angeles office of Latham & Watkins LLP.
Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the attorneys listed below or the attorney whom you normally consult.

A complete list of our Client Alerts can be found on our Web site at www.lw.com.

If you wish to update your contact details or customize the information you receive from Latham & Watkins, please visit www.lw.com/resource/globalcontacts to subscribe to our global client mailings program.

If you have any questions about this Client Alert, please contact Roxanne E. Christ or Brian J. Fox in our Los Angeles office or any of the following attorneys.

**Brussels**
Andreas Weitbrecht  
+32 (0)2 788 60 00

**Chicago**
Marcelo Halpern  
+1-312-876-7700

**Frankfurt**
Marcus Herrmann  
John D. Watson, Jr.  
+49-69-60 62 60 00

**Hamburg**
Joachim von Falkenhausen  
+49-40-41 40 30

**Hong Kong**
John A. Otoshi  
+852-2522-7886

**London**
Luke Grubb  
+44-20-7710-1000

**Los Angeles**
Roxanne E. Christ  
Brian J. Fox  
+1-213-485-1234

**Milan**
David Miles  
+39 02-3046-2000

**Moscow**
Anya Goldin  
+7-501-785-1234

**Munich**
Jörg Kirchner  
+49 89 20 80 3 8000

**New Jersey**
Monica Y. Awadalla  
+1-973-639-1234

**New York**
Hanno F. Kaiser  
John J. Kirby, Jr.  
+1-212-906-1200

**Northern Virginia**
Kevin C. Boyle  
+1-703-456-1000

**Orange County**
Patrick T. Seaver  
R. Scott Shean  
+1-714-540-1235

**Paris**
Olivier du Mottay  
Thomas Forshbach  
John D. Watson, Jr.  
+33 (0)1 40 62 20 00

**San Diego**
Scott N. Wolfe  
+1-619-236-1234

**San Francisco**
Kevin D. Burnett  
John M. Newell  
+1-415-391-0600

**Shanghai**
Rowland Cheng  
+86 21 6101-6000

**Silicon Valley**
Peter F. Kerman  
Patrick A. Pohlen  
+1-650-328-4600

**Singapore**
Michael W. Sturrock  
+65-6536-1161

**Tokyo**
Michael J. Yoshii  
+81-3-6212-7800