INFORMATION PRIVACY IN VIRTUAL WORLDS: IDENTIFYING UNIQUE CONCERNS BEYOND THE ONLINE AND OFFLINE WORLDS

TAL Z. ZARSKY*

I. INTRODUCTION

Online virtual gaming communities are evolving into an intriguing phenomenon, which is provoking legal scholars to acknowledge the unique legal issues associated with the proliferation of this technology.[1] As online virtual worlds consist of ongoing, digital interactions among many individuals, it is only natural that legal scholars will inquire into how personal information is collected and used within this realm.[2] In this Essay, I analyze how information privacy concerns are implicated by the expansion of online virtual worlds.[3] In doing so, I intend to address both the information privacy and gaming communities. I will introduce the information pri-

* Resident Fellow, The Information Society Project, Yale Law School. I thank Jack Balkin and the fellows of the Information Society Project for their comments and suggestions. I also thank the contributors to the terranova blog who provided me with much needed feedback and ideas, and Dan Hunter for facilitating my participation in the blog's discussion. Special thanks to James Grimmelmann, Beth Noveck, and Cory Ondrejka for comments on previous versions of this paper.

1. For recent examples, see F. Gregory Lastowka & Dan Hunter, *The Laws of the Virtual Worlds*, 92 CAL. L. REV. 1 (2004); *see also* EDWARD CASTRONOVA, VIRTUAL WORLDS: A FIRST-HAND ACCOUNT OF MARKET AND SOCIETY ON THE CYBERIAN FRONTIER (CESifo Working Paper Series No. 618, 2001), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=294828 (last visited Oct. 10, 2003). For an extensive list of online and offline sources regarding games, see the bibliography formed by Richard Bartle, *Designing Virtual Worlds: The Web Site*, *at* http://mud.co.uk/dvw/bibliography.html (last modified June 17, 2003) (providing an extensive list of online and offline sources regarding games in the virtual world).

2. I am unaware of other writings and research on this specific issue. The issue of privacy in virtual worlds was referred to in passing in Lastowka & Hunter, *supra* note 1, at 72 n.386, as an issue worthy of further inquiry.

3. To a certain extent, the following analysis echoes an inquiry that is carried out time in again in the Cyberlaw context: whether the new technology presents novel legal challenges, and what such challenges might teach us. For earlier versions of this inquiry in other contexts, see Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 111 HARV. L. REV. 500 (1999).

vacy community to a new world and technology that allows them to approach the "classic" privacy arguments in novel ways. I will also bring those interested in virtual worlds into the ongoing information privacy discourse and suggest several ways in which information privacy issues can apply to virtual worlds. Even though courts have yet to encounter the problems addressed below, I suspect these issues will arise in the near future as more users begin to utilize virtual worlds and as these worlds become more commercialized.

In Section I, I begin by describing several emerging technologies and the privacy concerns they generate. Next, I address the emergence of virtual worlds, and explain why they present novel legal and social issues. In Section II, I bring these two elements together, while examining whether virtual worlds present privacy issues that are worthy of an independent legal discussion. In so doing, I address the central privacy concerns arising from the use of these new applications and establish that they are substantially different than those unfolding in the "general" online world. Within this analysis, I focus on concerns stemming from the use of data exclusively collected (and thereafter used) within the gaming realm that is not aggregated with or connected to external factors (information which I define below as "Player Data"). Finally, in Section III, I address a popular approach toward solutions to the problems of online privacy — the *market-based solution* — and examine whether it is suited to virtual world privacy concerns. I conclude that the inherent structure of virtual worlds and the virtual worlds market will impede on users' ability to effectively signal their privacy preferences. Virtual worlds, however, will also provide users with powerful tools to spread ideas and opinions, thus potentially undermining unfair practices, abuses of data and market failures.

II. Privacy in Virtual Worlds — Is a Specific Discussion Necessary and Required?

A. *Prelude to Privacy*

Information privacy is generating a great interest in the public and policy discourse. A variety of popular and professional jour-

nals[4] have depicted, in great detail, the various forms of surveillance now available and the breaches of privacy to which they might lead. Initially, fears of surveillance and other privacy concerns have focused on the state that could potentially abuse its overwhelming power to intrude on the individual's rights.[5] This fear has been fueled by both actual instances of abuse[6] and cultural influences, such as Orwell's "1984"[7] that powerfully framed the paradigm of the state as the "Big Brother" that sees all.[8] Recent literature and trends in public opinion[9] have identified an additional source of concern — large and powerful commercial entities. In today's world, these entities reach almost every corner of our lives and have the ability to collect vast amounts of personal information and use this data in detrimental ways.[10]

4. *See, e.g.*, David Shenk, *Watching You: The World of High-Tech Surveillance*, NATIONAL GEOGRAPHIC, November 2003.

5. *See, e.g.*, DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 275 (2003).

6. For instance, in the U.S., the stories surrounding Watergate led to the enactment of the Privacy Act of 1974.

7. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

8. Some scholars believe the "Big Brother" metaphor is unsuitable to describe today's privacy concerns. *See, e.g.*, Daniel J. Solove, *Privacy and Power, Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1391, 1419-30 (2001) (arguing why a "Kafkaesque" metaphor is preferable).

9. For a glimpse of the public opinion on this issue, see *Opinion Surveys: What Consumers Have to Say About Information Privacy: Hearing Before the Sub. Comm. on Commerce, Trade and Consumer Protection of the House Comm. on Energy and Commerce*, 107th Cong. 17-19 (2001) (prepared statement of Alan F. Westin) [hereinafter *Opinion Surveys*]. *See also* Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV 1457, 1477-81 (2001).

10. *See* Tal Z. Zarsky, *Mine Your Own Business!: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 4 (2002-2003) [hereinafter MYOB]. The defining line between the state and private entities, and the specific fears of privacy they generate, is constantly blurring. Governments increasingly sell information about their citizens to commercial entities, and in some cases require commercial entities to provide them with the personal information they collected. For a most recent example, see Matthew L. Wald, *Airline Gave Government Information On Passengers*, N.Y. TIMES, Jan. 28, 2004, at sec. 1, 16, regarding the transfer of personal information from the airlines to the government as part of the 9/11 investigation. *See also*, Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003). For a famous incident in which information gathered in an ice cream promotion was passed on to the selective service, see David Burnham, *Selective Service to Stop Use of Birthday List*, N.Y. TIMES, August 4, 1984, at sec. 1, 5.

New technological tools that facilitate the gathering of information in novel and sophisticated ways have greatly contributed to the increasing severity of today's information privacy problems and concerns.[11] Recent innovations include cameras capable of viewing through walls and microphones that listen in from afar.[12] In addition, advances in technology are leading to the ever-decreasing prices of simpler surveillance tools such as video cameras that are omnipresent.[13] Technology also facilitates new business practices and services that provide comfort on the one hand, yet ongoing information gathering on the other. Credit cards and other means of electronic payment provide users with convenience, but allow commercial entities to gather a variety of data concerning the timing, form and place of every transaction.[14]

Technological advances in surveillance mechanisms affect the privacy discourse in several ways. Privacy concerns are exacerbated by the advanced ability to collect information while invading individuals' privacy and personal space, and the fact that such tools are used to collect information. In addition, these advances affect the public's expectation of privacy. As new technological means of surveillance unfold, individuals acknowledge and acquiesce to the fact that they are constantly watched. By lowering the objective, and thereafter subjective, expectation of privacy, these technologies will ultimately affect the legal outcome as to whether specific acts of surveillance are to be construed as violations of privacy expectations, and therefore privacy rights.[15]

---

11. For a general discussion of technology and surveillance, see SOLOVE & ROTENBERG, *supra* note 5, at 306. R

12. *See* A. Michael Froomkin, *Cyberspace and Privacy: A New Legal Paradigm? The Death of Privacy?*, 52 STAN. L. REV. 1461, 1468 (2000). For more information on surveillance technologies, see REG WHITAKER, END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 80 (1999).

13. *See, e.g.*, Sabrina Tavernise, *Watching Big Brother; On This Tour, Hidden Cameras Are Hidden No More*, N.Y. TIMES, Jan. 17, 2004, at B1.

14. For further analysis, see Tal Z. Zarsky, *Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society*, 56 ME. L. REV. 13, 18 (2004).

15. *See, e.g.*, Katz v. U.S., 389 U.S. 347, 361 (1967) (holding that whether an expectation of privacy exists is a two-tiered process: one that examines whether the person has exhibited an actual expectation of privacy, and whether the expectation be one that society is prepared to recognize as reasonable). *See also*, SOLOVE & ROTENBERG, *supra* note 5, at 293. R

Technological changes that directly affect the privacy discourse proceed beyond surveillance applications, and include advances in the ability to store and retrieve information.[16] Through the use of sophisticated algorithms, new "data mining" applications enable information collectors to analyze efficiently vast amounts of personal data. When applying data mining tools, information collectors can finally take advantage of the vast databases of personal information that the new surveillance applications provide.[17]

The debate over information privacy (or the lack thereof) has generated a specific interest with regard to the Internet. While in the offline world, commercial entities gather a great variety of personal data about consumers, such data usually pertains to a *final transaction*, and is therefore limited. Online, however, website operators can track and record the user's every action. Thus, in the Internet realm, even the acts of browsers (pun intended), who may never make a purchase, are easily scrutinized.[18] Moreover, as the Internet is entirely "digital," transactions are constantly and effortlessly surveyed, recorded, and saved. The Internet also provides elaborate and sophisticated means to use the personal information that is constantly collected and aggregated. For instance, website operators have begun to retreat from "broadcasting" content to the masses, choosing instead to "narrowcast" tailored content for every user on the basis of personal information they have previously obtained.[19]

The systematic and extensive abilities to collect and use personal information will soon develop offline. With new forms of identifying applications, such as voice and face recognition, offline

16. An example for the use of such technological applications is Walmart. According to a 2002 report, there are 500 terabytes of data in Walmart's Bentonville data warehouse center (in comparison, the IRS has 40 terabytes stored). *See* Owen Thomas, *Lord of the Things*, *at* http://www.business2.com/b2/web/articles/0,17863,514502,00.html (last visited Sept. 9, 2004) (explaining how Walmart uses technology to accumulate vast amounts of data).

17. See MYOB, *supra* note 10, at 6-17, for a description of the various new means of data analysis.

18. This point is emphasized in Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198 (1998).

19. For example, the "Daily Me" is an analysis of one way of such tailoring. *See* MYOB, *supra* note 10, at 40 (The "Daily Me" refers to an online application that provides users with a personally tailored newsletter prepared according to their preferences). *See also* CASS SUNSTEIN, REPUBLIC.COM (2001).

surveillance practices will allow data collectors to register every move we make. Thus, as advances in technology continue, privacy concerns of the broader, physical realm will increasingly resemble those of the online world.[20]

B. Privacy in Virtual Worlds

1. General

Massively multi-player online role-playing games ("MMORPGs"), such as Ultima Online, Everquest, and The Sims Online ("TSO"), introduce players to vast communities in which they can engage in a variety of activities and communications over an extensive period of time.[21] Within these realms, users interact with the game controllers and each other through alter egos, or avatars.[22] As the use of these identities is consistent, avatars can accumulate wealth, power, and a reputation throughout the virtual community. Furthermore, while players invest both time and money in their virtual persona, they grow attached to it and see it as a reflection and even an important part of their physical, offline "selves."[23]

Structurally, almost all MMORPGs are operated and controlled by a central entity. This entity constantly maintains the virtual world, while charging users monthly subscription fees. The contractual relationship between the users and the game controllers is set out in an End-User License Agreement ("EULA") or the relevant Terms of Service ("ToS"). These agreements are typically accepted by the user upon installation of the relevant software or logging on to the game's website.[24] Such agreements address various aspects of the gaming experience, and include specific refer-

20. For two examples of new trends of meticulous surveillance in the world of brick and mortar, see Jennifer 8. Lee, *Welcome to the Database Lounge*, N.Y. TIMES, Mar. 21, 2002, at G1 (collection of personal information by pubs when swiping the driver's license of a patron); Stephanie Simon, *Shopping with Big Brother*, LOS ANGELES TIMES, May 1, 2002, at 1 (describing a store in which cameras follow shoppers throughout the store and register every move).

21. For a general description of such worlds, see CASTRONOVA, *supra* note 1, at 4. For a description of the evolution of this market, see *id.* at 9.

22. For the origins of this term, see CASTRONOVA, *supra* note 1, at n.3.

23. *See* Lastowka & Hunter, *supra* note 1, at 52 n.280.

24. *See, e.g.*, the Sims Online (Electronic Arts) EULA, which states: "*Your use of EA Online is subject at all times to our Terms of Service, our Privacy Policy and the AOL Name Terms of Use*," *at* http://www.ea.com/global/legal/tos.jsp (last visited Oct. 28, 2004).

ences to the companies' privacy policies.[25] The central entities that control the virtual environment are at times referred to as "wizards" or "gods" and with good reason; they can "wipe out" months of labor in seconds,[26] silence and abolish players from a game,[27] as well as create worlds and endow players with new powers.[28] In addition, these central entities can see and record everything users do within these worlds, and thus form a fertile ground for privacy concerns.

To demonstrate the privacy concerns virtual worlds introduce and their uniqueness, consider the following comparison to the sale of "regular" computer or console games[29] (which to a certain extent, resembles the differences between the perils of online and offline data collection). When purchasing a computer or console game, the seller or other information collectors are limited to registering and acknowledging the purchase of these specific products. Sellers cannot obtain information about who subsequently used the game or the extent of its use. With virtual worlds, however, a variety of additional personal data is available to the game operators: Information regarding the extent of play and the times and places the user is connecting and playing from. In addition, game operators can gather information about every specific move the user makes or word a player says within these virtual worlds — including facial and body gestures — store that information and subsequently tailor their interface with every user on the basis of their specific traits and needs.[30]

Another comparison to keep in mind when assessing virtual world privacy concerns is between these worlds and the general on-

25. *See, e.g.*, the Sims Online EULA, which states: "*We will not collect any personal information about you, however, without your knowledge and consent as stated in the EA Privacy Policy*," *at* http://tr.eagames.com/news/legal_pccdonline.jsp (last visited Oct. 28, 2004).

26. *See* Jack M. Balkin, *Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds*, VA. L. REV. (forthcoming 2005).

27. *See infra* Section III.

28. For a description and analysis of the powers of "wizards" or "gods" in virtual worlds, see Lastowka & Hunter, *supra* note 1, at 54.

29. For example, such games for Playstation and X-Box systems. Note that these forms of entertainment have shifted to a network environment as well — as they will now facilitate multiplayer games through the use of the Internet and other networks.

30. For instance, the game controllers can create and store a complete log of all activities and transactions in which the avatar participated, with whom the avatar "spoke" and what was said, every "land" the avatar entered (including the specific time and location), and furthermore, every "movement" the avatar chose to make.

line discourse. In virtual worlds, the collection of personal information and subsequent profiling could be carried out with greater efficiency. In the online realm, however, even though sophisticated forms of surveillance are available, information collectors face serious challenges when trying to create meaningful profiles about their users, as these profiles tend to be limited in scope and filled with errors. While website operators can successfully track a user's journey within their website,[31] they face difficulties aggregating and collating information from individuals using multiple machines, constantly logging in and out, or engaging in other online activities beyond their specific website. To overcome these difficulties, website operators employ advanced techniques, such as the use of "cookies,"[32] or requiring login passwords to every website. In addition and to enrich the profiles being formulated, collectors at times purchase information on secondary markets and integrate it with their own databases. Yet, when integrating the data collected at different times, places, and from different sources into a single profile, a great deal of information is lost or corrupted, as profiles are matched incorrectly, overlap, or are filled with irrelevant data. In virtual worlds, however, the process of creating and maintaining a profile is simpler and more effective, while the profiles created can be of a broader scope and present fewer errors. In terms of scope, virtual world profiles will include information pertaining to an extended online experience (rather than one specific website) that stem from data collection that is carried out over a prolonged period of time, and includes several forms of social interactions. In terms of errors, these profiles will not result from the complicated aggregation process described above, as a detailed profile could be derived from information collected about one avatar[33] by one game controller.

31. On the collection of "clickstream" data online, see SOLOVE & ROTENBERG, *supra* note 5, at 493. R

32. On the issue of "cookies," see *id.*

33. A caveat to the benefits of "virtual world" surveillance is that at times users sell their "avatar" to another person on a secondary market (via eBay or other designated websites). Therefore, even though game controls track the actions of an avatar, they might not be correctly tracking the actions of a single individual (I thank James Grimmelmann for this insight).

2. Why the Analysis of Virtual Worlds is Interesting and Important

A skeptical reader might acknowledge that virtual worlds portray unique privacy issues and concerns, yet remain unconvinced about the importance of specifically addressing this arguably esoteric world of online gaming. To such skeptics, I provide several responses.

First, the phenomenon of MMORPGs and virtual worlds is far from esoteric. Several MMORPGs attract well over 100,000 players,[34] and according to some estimates formulate an internal economic market larger than Bulgaria's.[35] The revenue generated by the sale of games (in general) exceeds Hollywood box office revenue in the U.S. market,[36] and is rapidly growing. Virtual games are now appealing to a broad demographic. Gamers are both male and female and of various backgrounds and ages.[37] It is true that, as a cultural phenomenon, virtual worlds lag behind the more popular forms of entertainment, such as television and cinema.[38] In certain countries and cultures, however, virtual games are becoming an influential pastime. In South Korea (with its powerful broadband infrastructure), for instance, gaming has reached unprecedented popularity, and successful gamers often attain rock star status.[39] If

34. Everquest, for example, is the most popular virtual game in the U.S. with over 420,000 monthly subscribers. *See* Lastowka & Hunter, *supra* note 1, at 26. For additional information regarding number of subscribers, see CASTRONOVA, *supra* note 1, at 2 & n.1, 11.

35. For one reference to this fact, see Ania Lichtarowicz, *Virtual Kingdom Richer than Bulgaria*, BBCNEWS, March 29, 2002, *available at* http://news.bbc.co.uk/2/hi/science/nature/1899420.stm. Note, however, that the source of comparison is GDP. As Bulgaria's population is greater, its economy is in fact considerably larger (I thank James Grimmelmann for this observation). For a recent discussion as to the comparison between economies of states and virtual worlds, see Edward Castronova, *Virtual World Economy: It's Namibia, Basically*, Terra Nova, *at* http://terranova.blogs.com/terra_nova/2004/08/virtual_world_e.html (Aug. 3, 2004).

36. *See* James M. Pethokukis, *Screen Wars*, USNEWS & WORLD REPORTS, Dec. 16, 2002, at 38-39.

37. *Id. See also* Amy Harmon, *A Real-Life Debate on Free Expression In a Cyberspace City*, N.Y. TIMES, Jan. 15, 2004, at A1 (referring to the fact that 60% of the Sims subscribers are women).

38. *But see* Lastowka & Hunter, *supra* note 1, at 5, for indications to the contrary in other countries.

39. *See* Mei Fong, *Don't Tell the Kids: Computer Games Can Make You Rich, Players in South Korea Do It Full Time, and Lucky Few Have Six-Figure Incomes*, WALL ST. J., May 21,

these trends spread and migrate, the issues at hand will certainly become ever more relevant and significant.

Second, privacy questions in MMORPGs are of interest and importance because analyzing virtual worlds offers a glimpse into what tomorrow's online environment might resemble. As explained above, virtual worlds facilitate the collection of personal information about a specific user throughout the entire online gaming experience. These collection capabilities might spread to the broader online environment as well. Recent trends in online business strategies are featuring a shift towards the dominance of mega-websites that offer a variety of online services to every specific user.[40] These sites are at times referred to as "walled gardens" as they aim to entice the user to remain within the boundaries of this specific site that can provide the user with all the various sources he or she might require. A direct result of such new practices will be the ability to create efficiently a more distinctive and complete profile of every user's online conduct. This profile could be applied to tailor future interactions between users and the walled gardens, and thus exacerbate privacy concerns.[41] Virtual worlds allow us to catch an early glimpse of the problematic privacy aspects of tomorrow's walled gardens, and get a head start in constructing proper solutions.

Finally, the societies created within these virtual realms have emerged out of thin air, and are not subject to the constraints of the physical world. Within these societies, there is no scarcity or shortage of resources (unless such scarcity is intentionally built into the system).[42] Furthermore, since users interact in these realms without revealing their nationality, race, or personal appearance, these worlds are relatively free of animosity and biases that are re-

2004, at A1. Note that this story does not refer to MMORPGs, but faster, shorter, and more violent games.

40. Here, I refer to mega-websites such as AOL or Yahoo! that strive to provide several services–such as travel, email, search engines, job searches, and others. It should be noted that this model would suffer substantial setbacks if users learn how to use independent search engines such as www.google.com.

41. *See* MYOB, *supra* note 10, at 34-42, for an analysis of this issue.

42. *See* CASTRONOVA, *supra* note 1, at 17, for a discussion of scarcity in virtual worlds.

lated to these attributes.[43] Thus, researching[44] these environments serves as a fertile ground for the analysis of utopian societies and an interesting contrast to our own. Examining privacy problems and suggesting possible solutions in this realm will also allow policymakers to "beta test" legal regulations and social regimes before transferring these ideas to the "brick and mortar" or even the Internet realm, where the stakes of failure are considerably higher.[45]

III. VIRTUAL WORLDS — UNIQUE PROBLEMS?

A. General

In this Section, I examine whether privacy questions arising in virtual worlds lead to unique legal problems. At first blush, it seems as if privacy concerns arising when addressing virtual worlds resemble those evident in the "general" Internet environment, and that a separate analysis is therefore redundant. Indeed, there are many similarities among these subtopics. The Internet resembles the networks MMORPGs create, and virtual games are usually accessed and played through the web. Virtual worlds allow the same form of meticulous collection of information, as well as the use of such personal data to carry out specific tailoring for every user. A closer analysis of the MMORPGs environment,[46] however, indicates several key differences.

At first, several key differences between the general online and the specific MMORPGs environments indicate that virtual worlds present *fewer* privacy concerns. One such difference pertains to the actual personal information that is collected within virtual worlds. While game controllers can gather precise data regarding the players' actions, much of this information is meaningless to the online

43. For an in-depth analysis of the interplay between racism and the environment the Internet creates, see Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1130 (2000).

44. *See generally supra* note 1. In addition, for a list and discussion of the recent broadening of academic research concerning Virtual Worlds, see Terra Nova blog discussion *at* http://terranova.blogs.com/terra_nova/2004/01/virtual_worlds_.html (last visited Oct. 4, 2004).

45. For an in-depth analysis of the applicability and suitability of rule testing in virtual worlds, see Caroline Bradley & A. Michael Froomkin, *Virtual Worlds, Real Worlds*, 49 N.Y.L.SCH. L. REV. 103 (2004).

46. For a comparative analysis of various virtual worlds, see Bruce Sterling Woodcock, *An Analysis of MMOG Subscription Growth — Version 10.0*, *at* http://pw1.netcom.com/~sirbruce/Subscriptions.html (last visited Oct. 4, 2004).

marketer and advertiser. The majority of MMORPGs are set in worlds of fantasy, in which the users interact as elves or warriors. Therefore, it would be quite difficult to draw inferences from these worlds to consumer preferences in the offline realm. While it is true that this data could be applied toward a search for correlation between virtual world activities and "physical world" consumption, such analysis will be detached from decades of empirical studies of marketing and consumer behavior, and therefore of lesser value.

An additional argument as to the decreased severity of privacy troubles in virtual worlds concerns the clear contractual framework and relationship between the user and the game controller. Since the EULA or the ToS govern most interactions between the user and game controller (as well as between the users themselves), virtual worlds will rarely involve "open-ended" privacy questions, and most issues will be directly addressed within this legal framework. Nevertheless, the existence of the overall contractual framework should not end the virtual world's privacy analysis, but only provide a starting point. Questions will still arise when privacy concerns pertain to third parties that are not privy to the relevant agreements. Privacy issues also arise when the specific privacy concern is *not* addressed in the relevant agreement (although the contractual framework would be constantly modified to reflect new privacy concerns). Most importantly, issues that are addressed in the specific agreements can still present open-ended questions if legislation deems the relevant contractual provisions unenforceable.[47] Such unenforceability may stem from the unfairness of the agreement or the fact that its provisions are contrary to public policy. As in other market settings, the virtual worlds' market could include consumer protection rules that intervene in contractual relationships between parties, and set immutable or default rules. I do not intend to provide a legal analysis of the instances in which the terms of the EULA must be disregarded or changed in view of unfair privacy practices, nor address the intricacies of contract law. To sufficiently address this matter, the analysis must not only establish the privacy wrongs

47. Lastowka & Hunter, *supra* note 1, at 50-51, make a similar point with regard to the EULA's provisions concerning property rights, and whether they could be challenged or circumvented by claiming they are too restrictive. In addition, see Balkin, *supra* note 26, at 25, for a similar argument, while referring to instances in which the EULAs promote fraud. R

carried out, but also the appropriate test for contract validity that will vary in accordance with the specific state law applying to every case. I do, however, address several instances in which legislators and courts may decide to set the virtual world's contractual framework aside in view of other policy considerations. Thus, despite the omnipresence of the EULA in virtual worlds, a discussion regarding problems of information privacy is nevertheless warranted.

To identify the unique privacy issues virtual worlds create, I suggest we consider two distinct categories:

1. Privacy concerns that arise from a breach in the crucial connection between the virtual world and the physical world. This category presents questions that, though troubling, bear a striking resemblance to those arising in general privacy law especially in the online context; and

2. Privacy concerns that do not involve the flow of information between the physical and virtual worlds, but exclusively pertain to the collection, analysis, and use of "personal" information within the virtual realm. This latter category provides the majority of interesting questions that are unique to virtual worlds.

B. Privacy Concerns and the Link between the Virtual and Physical World

Here, I confront the most basic and apparent privacy-based fear virtual worlds generate: That the "veil" separating the players' action when interacting in virtual worlds, and their actions and identity in the physical world, might be pierced with personal information leaking in both directions. In this context, we confront the "usual suspects" of privacy law: the government, other individuals interacting in "game space," and the entities controlling the game.

The government's collection and use of personal information in virtual worlds, and its subsequent attempts to connect the virtual and physical identities, can lead to several forms of privacy concerns.[48] Generally, a government may be interested in linking the virtual and physical identities of users to sanction the "physical" per-

48. Clearly when considering information privacy in the context of law enforcement, the implications of collecting and using personal data go beyond those in existence in the "commercial" world and include fears of tyranny and the stifling of personal liberty. On the fears and implications of surveillance by law enforcement, see SOLOVE & ROTENBERG, *supra* note 5, at 275. **R**

son for the actions of his or her online identity.[49] In addition, this link may be important to investigate or prevent illegal or illicit actions planned in one world, and carried out in the other. To establish this "link," government agents may gather information by simply maintaining a presence in a virtual world and collecting information as any other player observing the ongoing interactions. Thereafter, the government could analyze this data and, should it generate suspicion or present actual criminal acts, try and deduce the identity of the offline persona that stands behind the online avatar from the data gathered in virtual space. In these instances, the observed avatars/persons can rarely argue that their privacy has been breached, as the information the government collects and uses was viewed and gathered in an open, public forum where an expectation of privacy can rarely exist.[50] The situation may be somewhat complicated should government agents refrain from properly identifying themselves or their assignment, yet these problems closely resemble situations addressed at length in the online and offline setting, and therefore are not unique.[51]

Governments can also reveal the link between the physical and the virtual world identities of users by requiring game controllers to surrender this information to them directly.[52] Again, the issue emerging, though important, is far from unique. An analysis of these issues will echo the ongoing debate regarding the rights and

49. A sanction that is limited to the actions of the "avatar" might be insufficient, as it is limited to the assets and reputation of the avatar, while at times the severity of the crime requires limitations on the freedom and punishment of the "physical" persona as well.

50. On this issue, note the language of the ToC of The Sims Online stating: "*You acknowledge and agree that your communications with other users via chats, conferences, bulletin boards, and any other avenues of communication on this Service are public and not private communications, and that you have no expectation of privacy concerning your use of this Service*," *available at* www.ea.com (last visited Oct. 28, 2004). For a discussion as to the existence of an expectancy of privacy in public spaces, see Zarsky, *supra* note 14, at 19. *See also* SOLOVE & ROTENBERG, *supra* note 5, at 70. R R

51. This situation has arisen several times in the general online and chatroom context. *See, e.g.*, United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997) (holding that the openness of the chatroom diminished the defendant's expectancy of privacy).

52. For anecdotal evidence as to the use of such information in South Korea, see Terra Nova blogs discussion, *at* http://terranova.blogs.com/terra_nova/2003/10/privacy_and_vwss.html (reference to the use of such information to find a runaway girl and locate army deserters).

duties of ISPs and other Internet service facilitators to provide the government with this form of identifying information, and the government's right to request (or demand) it.[53] Furthermore, in view of recent security concerns, EULAs will surely detail the instances in which the game controllers can provide the government with such information, thus simplifying a problem that is sufficiently addressed in the wider, online context.

Beyond the acts of government, privacy concerns in this context may originate from the actions of other players. Such players may learn of the hidden connection between the virtual persona and the physical player by deducing it from data they gather while playing, or by receiving this information directly from the game controllers.[54] Thereafter, they might publicize such information, while causing another player grief or damage. As before, the questions arising are far from unique and exist outside the gaming environment.[55] In a long string of cases and in a variety of settings, plaintiffs have argued (with mixed success) that others have exposed personal information that they tried to conceal, which has resulted in losses and grief. Yet in this context and as opposed to the conventional online setting, privacy concerns may arise as a result of the flow of personal information in *both directions* of the critical nexus between the online and offline world. Here are two examples to explain this point.

A simple case is the one of Player *A* — an average citizen who does not want his offline friends and neighbors to learn of his escapades in virtual worlds, where he portrays a grotesque avatar. Player *A* hides his physical identity when interacting in virtual worlds, and when other players publicize offline the connection between him and his avatar, he is infuriated and considers such acts a breach of privacy. This scenario resembles other online instances

53. The relevant process for obtaining such information from ISPs is set forth in ECPA, 18 U.S.C. § 2703(c)(1)(B). For an analysis of these sections, see SOLOVE & ROTENBERG, *supra* note 5, at 327. **R**

54. Note that as virtual worlds become more complex and elaborate, these problems will surely exacerbate. In Second Life, for example, players are able to construct surveillance mechanisms and "install" them within the game, and thus allow them to "spy" and follow other players with greater precision (I thank Cory Ondrejka for this insight).

55. *See infra* note 65 for a reference to these cases. **R**

where private facts regarding the surfing patterns of "physical" individuals are revealed in public.

Yet, virtual worlds can pose the opposite problem as well. In MMORPGs, players invest a great deal of time and money in creating and maintaining online reputations. As this virtual persona might be very different from their physical selves, users might consider information regarding their offline lives, jobs, gender, or age as harmful to their virtual reputations.[56] To illustrate this point, consider Player *B* — another average player who is interested in hiding where she lives and information regarding her job from her virtual friends, as she fears she might appear too boring or different than the virtual identity she constructed. When other players begin discussing and disclosing information about her actual address, job, and appearance within the virtual world, Player *B* is offended and views these actions as a breach of privacy. In this example, we are introduced to a unique privacy concern — the privacy of the avatar — that emerges as a result of the creation of online reputations and identities that are detached from the physical self.[57]

Whether the "leakage" of personal information regarding the various identities would or should constitute a privacy tort requires a case-by-case analysis. When information about users is revealed in the "parallel world" without their permission or approval, such actions may amount to a breach of the "Public Disclosure of Private Facts" tort. This tort, which is stated in the Restatement and accepted in many states,[58] is notoriously hard to prove,[59] and requires the plaintiff to establish that the matter disclosed was "highly offensive to a reasonable person" and is "not a legitimate concern to the

56. For a most recent example in the "Sims Online" realm, see Jim Schaefer, *Sex and the Simulated City: Virtual World Raises Issues in the Real One*, DETROIT FREE PRESS, Jan. 27, 2004, *available at* http://www.freep.com/news/mich/sims27_20040127.htm. In this case, a player disclosed the physical identity of another player–who had assumed the role of "female prostitute" in the virtual realm. Eventually it was revealed that this player was in fact a 17 year old boy — which obviously affected the way he was thereafter treated in the virtual world.

57. Such conduct is addressed in the Second Life Community Standards, which according to the contractual framework the players enter, must be fully abided by. *See* http://secondlife.com/corporate/community.php

58. *See* SOLOVE & ROTENBERG, *supra* note 5, at 18. R

59. *See id.* at 126.

public."[60] In addition, this tort stands in contrast to the free speech rights of those disclosing the information about the virtual/physical persona.[61] The relevant case law that applies to the tort "offline" should apply to the virtual world's scenario,[62] and also might lead to a legitimate legal cause of action for transferring personal information from the physical world to the virtual one. Should this tort apply in virtual worlds, plaintiffs — such as Player *B* — will be required to establish the above elements of the tort, and the courts should examine whether virtual worlds create separate identities and separate reputations that should be preserved through the creation of specific legal rights.

Returning to the overall analysis of privacy concerns we reach the final category, in which concerns arise from the actions of game controllers that reveal or use information regarding the crucial nexus between the physical and virtual identity. Again, these specific practices may indeed prove problematic yet resemble complaints and subsequent legal debates set in the online realm regarding the actions of ISPs and websites selling or misusing their users' personally identifiable data.[63] If courts or regulators are con-

60. *See* RESTATEMENT (SECOND) OF TORTS § 652D, PUBLICITY GIVEN TO PRIVATE LIFE (1997) ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.").

61. *See generally* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop Others from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

62. See Zarsky, *supra* note 14, at 50, for an analysis of this tort. For a famous example where plaintiffs failed in their suit against the press arguing this tort, see Sipple v. Chronicle Publishing Co., 201 Cal. Rptr. 665, 670 (Cal. Ct. App. 1984). For a description of the facts of this case see ROSEN, THE UNWANTED GAZE- THE DESTRUCTION OF PRIVACY IN AMERICA 47-48 (2001). *See also* Sidis v. F-R Publishing Corp., 113 F. 2d 806 (1940). For a description of the facts of this case, see SMITH, *supra* note 6, at 224. **R** **R**

63. For an example in the general "online" context, see complaints against DoubleClick regarding their plans to merge their DART database with that of an offline personal database, see Greg Miller, *DoubleClick Cancels Plan to Link Net Users' Names, Habits; Internet: Protests Prompt Firm to Halt Project To Combine Databases, Which Could Threaten Web Surfers' Anonymity*, LOS ANGELES TIMES, Mar. 3, 2000, at C1; Bob Tedeschi, *In a Shift, DoubleClick Puts Off Its Plan for Wider Use of the Personal Data of Internet Consumers*, N.Y. TIMES, Mar. 3, 2000, at C5. Another example of potential database misuse is the RIAA's request of Verizon to disclose names of specific users that were allegedly infringing copyrighted materials by swapping files online. *See* Amy Harmon, *Verizon Ordered to Give Identity of Net Subscriber*, N.Y. TIMES, Jan. 22, 2003, at C1.

fronted with issues concerning virtual world privacy in this context, their analysis must account for and balance the unique and contradicting elements virtual worlds bring into play, including: (1) the fact that clickstream data in virtual worlds could be aggregated and analyzed with greater efficiency and ease (leading to the formation of broader databases), (2) that the information collected in virtual worlds mostly pertains to preferences that are somewhat detached from the physical world, and therefore perhaps less significant and revealing, and (3) that the game operators' actions would usually be addressed in a detailed contract the users agreed upon.

C. Privacy Concerns and the Collection and Use of Information Exclusively Within Virtual Worlds

1. The Significance of "Player Data"

Beyond issues that pertain to the "leakage" of information between the "offline" and "online" worlds, virtual worlds present unique privacy implications resulting from the collection and use of personal information exclusively within the virtual worlds. Here I refer to personal information that is collected online and is not linked to any specific attribute of the "physical" user, but only to the virtual avatar. In other words, I address instances in which the game controllers concede to refrain from linking the information they collect in "game space" to any form of information that identifies or pertains to the "physical" user such as the user's name, address, zip code, or information associated to methods of payment.

Nevertheless, even within this relatively limited scope, game controllers have the ability to collect vast amounts of interesting data about every user. They can gather data pertaining to the times of the day the player engages in play in general and specific virtual activities in particular, the parts of the virtual world the user visits and the goods she buys, exchanges, and consumes, the other avatars he or she chooses to interact with and the times they do so (information I will refer to as "player data").[64] The analysis and use

64. A problem that may arise through the analysis of "player data" is the use of information previously collected in sites and games mostly used by children. I will not be addressing this specific problem in my analysis. This analysis must take into account specific laws and regulations, which pertain to this matter. *See, e.g.*, Children's Online Protection Act, 15 U.S.C. § 6501 et seq.

of such player data leads to a specific set of privacy concerns that are different from those surfacing in the general "online world" under similar circumstances.

The distinction between "player data" and other forms of personal information that are directly linked to the "physical" individual is not unique to the gaming setting. A similar distinction between identifiable personal information (IPI) and non-identifiable personal information (non-IPI) has been drawn out in several contexts of privacy law. In one context, IPI is defined as "data used to identify, contact or locate a person, including name, address, telephone number, or E-mail address," and non-IPI is defined as:

> [N]ot linked to a particular person and is typically compiled from click stream information compiled as a browser moves across different Web sites (or a single Web site) serviced by a particular network advertiser or from information provided by third parties (so long as that information is not personally identifiable to the network advertiser).[65]

Similar distinctions are drawn out in various privacy policies[66] and settlement agreements governing the use of personal information in the online setting.[67] Overall, non-IPI is afforded a lower level of privacy protection.[68] When addressed by regulators, it is treated with suspicion in view of the fear that it would be aggregated with other IPI databases, and thus traceable to a specific individual, and rarely with regard to the use of such data on its own.

---

65. See the NAI website *at* www.networkadvertising.org.

66. *See, e.g.*, In the Matter of DoubleClick Inc., Agreement between The Attorneys General of the States of Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington and DoubleClick Inc., Aug. 26, 2002, *available at* http://www.oag.state.ny.us/press/2002/aug/aug26a_02_attach.pdf (last visited Oct. 7, 2004) (see section § 12 for the definition of "Automatic User Data").

67. In the EU, a similar distinction is drawn out, while data addressed above as IPI is usually considered as "Personal Data," which is defined in Article § 2(a) of the EU Data Protection Directive, and awarded a higher level of protection. This definition of "Personal Data" refers to "any information relating to an identified or identifiable natural person." *See* SOLOVE & ROTENBERG, *supra* note 5, at 721-24. R

68. The protection of non-IPI will amount to an "opt out" option, at the most. *See, e.g.*, *supra* note 64.

Identifying privacy concerns stemming from the use of "player data" is an uphill battle. Many of the rationales for curbing the collection and analysis of personal information are significantly weakened when solely applied to non-IPI. Generally, the salient arguments against online data collection and profiling are that they cause the observed individual to engage in self-monitoring, act in a conforming manner,[69] and refrain from forming intimate relationships.[70] In addition, profiling has been criticized for reinforcing existing stereotypes and behaviors.[71] Yet, it is difficult to state these arguments when opposing the collection and use of player data in virtual worlds. In this context, collectors cannot identify the physical person being monitored, thus weakening the argument that such monitoring adversely affects the monitored individual's state of mind. If users know they are watched in the virtual world, but cannot be identified outside it, they will not be inclined to alter their offline behavior in view of this form of ongoing surveillance. In addition, as the avatar is detached from the physical persona, its description need not include the specific attributes that are commonly the basis for animosity and bias (unless the user intentionally chooses such attributes), thus limiting the fears of stereotypical and other forms of unacceptable discrimination in game space.[72]

Yet, there is more to "player data" than meets the eye. When users interact within virtual worlds, they do so over long periods of time and while using a consistent persona — two important elements that lead to the accumulation of rich and diverse data in the hands of game controllers. In addition, MMORPGs allow users to interact in a world that offers a broad set of experiences where they can exercise a variety of personality traits and preferences. In view of these unique factors, we must reconsider the overall lenient attitude toward the collection and use of non-IPI when addressing the "virtual world" setting. To identify and articulate the unique prob-

69. *See* Julie E. Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1379 (2001) (stating the importance of having unmonitored choices).

70. *See* Kang, *supra* note 18, at 1212. **R**

71. Oscar Gandy, Jr., *Exploring Identity and Identification in Cyberspce*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 1085 (2000).

72. Note, however, that in virtual worlds, there is still the possibility of discrimination against "virtual minorities" (i.e. avatars that chose to define themselves as such) that reinforces negative social norms. *See* Balkin, *supra* note 26, at 43. **R**

lematic outcomes of "player data" analysis and use, I address two possible arguments: One that requires that we recognize the importance of the new identity emerging in virtual worlds, while the other practically demonstrates how the collection and use of player data could prove to be harmful.

2. Player Data and the Avatar Identity

Recent scholarship addressing virtual worlds and other online communities promotes the notion that when players devote hours to interacting in these realms, not only are they creating an alternative social network, but also a new identity for themselves. Such scholarship also states the importance of these new extensions of the self that allow users to search, explore, and broaden their individual identity.[73] Moreover, for some players their online "avatar" identity proves to be more central and essential than their "physical" one.[74] According to this perspective, if the "virtual" identity is socially significant and important, it should be entitled to independent privacy rights. The rationales for creating such rights in virtual space will echo those voiced when deliberating on the importance of privacy in the "brick and mortar" world, namely, that the virtual identity must be protected from surveillance to prevent self-monitoring, conformity, and other troubles associated with constant data collection.

In this Essay, I refrain from pursuing the "virtual identity" rationale for adopting stricter privacy practices that will pertain to "player data." It is still too early to establish whether "virtual personas" should be considered as extensions of the "self," and consequently, provided with privacy rights during their online discourse. Establishing the importance of "virtual identities" is a highly subjective task and will vary among players and player communities. Additional time is required until a consensus forms regarding the

73. *See* SHERRY TURKLE, LIFE ON THE SCREEN 203 (1995). When discussing the use of MUDs (an early version of today's virtual worlds), Turkle argues that they provide users with a "psychological moratorium." In addition, Turkle mentions that "*The moratorium facilitates the development of a core self, a personal sense of what fives life meaning.*" *Id.* at 263.

74. *See* Lastowka & Hunter, *supra* note 1, at n.280 (quoting Castronova's research indicating that for thousands of players, the virtual realm was their true home).

existence and extent of this separate identity and its respective rights.

3. Specific Detriments Arising from the Analysis of "Player Data"

Beyond the claims premised on the importance of the virtual identity, "player data" should be treated with additional caution in view of the potential detriments and concerns that may arise from its collection and subsequent use. To understand these detriments and concerns, this Section examines several uses of player data by the game controllers. Generally, player data could be applied to a great many uses, ranging from malicious acts to problematic business practices. I choose, however, to address actions that fall within the main objective of any online gaming company — increasing its revenues through legitimate business practices. To achieve revenue growth, the firm can utilize its "player data" database to meet two specific objectives: (1) assuring that players remain faithful customers and engaged in the game (and even increase their playing time); and (2) adding new revenue sources by introducing retail and direct advertising schemes. Below I examine how player data is and could be applied to meet these objectives. At this time, some of the practices I describe are only conjectural. Nonetheless, I expect that they will grow common in the near future, and lead to unique privacy concerns. The necessity of an analysis of these practices and the possible uses of player data at this early juncture is to fully address the implications before business practices become institutionalized norms.

a. Data collection, churn reduction, and excessive playing

One possible use of "player data" by game companies will focus on reducing "customer churn" and assuring that players do not quit the game. As the competition among game companies for each subscriber grows fierce, firms will become strongly motivated to use all means available to maintain their customer base. Therefore, game operators will use player data to encourage players to maintain and even increase their involvement in the game, both in terms of time and financial investment. Here, the cautious reader might

argue that it is unclear whether gaming companies are indeed interested in encouraging players in that way, as most MMORPGs use a "fixed fee" policy, according to which players are charged a set fee regardless of the their actual playing time or level. Therefore, firms have no reason to encourage players to engage in extensive play, as intensive players are consuming valuable memory, bandwidth, and other resources without providing additional revenue. Yet, this assertion is untrue. Gaming companies are interested in extensive playing by involved players, as these players and such involvement cause virtual worlds to flourish, create a vibrant community, and in that way attract new players (and therefore revenue sources). In addition, game companies are constantly introducing new pricing schemes and models in which players pay extra fees for additional resources or improved access and quality. Thus, the firms can directly benefit from the players' increased involvement.[75] Finally, it is possible that in the future gaming companies will introduce scaled pricing schemes that will differentiate among players on the basis of the specific "playing plan" they decided to purchase. In these cases, firms will have a direct interest in increased player involvement.

To encourage players to increase (or at least maintain) their involvement in a virtual world, game companies will closely monitor their users' playing patterns in an attempt to establish which patterns of behavior lead to enhanced playing, and which lead to exiting the game (or "customer churn").[76] They will further examine this information to establish the most successful incentives for motivating different groups of players. After identifying these crucial factors, game controllers will apply them to specific users by examining their respective personal profile and manipulating the gam-

75. For example, some games generate income from the sale of "extension" packages that provide their purchasers with additional privileges in gaming space (such as additional features, accessories and easier access to new worlds). *See, e.g.*, Michael Learmonth, *Virtual Real Estate Boom Draws Real Dollars*, USA TODAY, June 8, 2004, *available at* http://www.usatoday.com/tech/webguide/internetlife/2004-06-03-virtual-realty_x.htm (describing Second Life allowing players to generate additional income through the sale of additional land to interested players).

76. For a discussion of "churn analysis" and the importance of data mining applications for this process, see MYOB, *supra* note 10, at 6-17.

ing environment to assure that players are satisfied.[77] For instance, they might strategically increase the value of a struggling player's assets, or create situations and realities in which the player encounters additional assets or points so to enhance their motivation.[78]

The analysis thus far is still lacking several crucial components. First, it does not illustrate how these supposed problems are unique and any different than those of the online world in general. Online, websites can manipulate their users' environment and interface as well, while using the personal data accumulated about the specific users during their interaction within the website.[79] Second, the analysis does not address any detrimental outcomes stemming from the game operator's actions — as players should be considered as autonomous agents that can decide to play or stop playing at any time.

Yet the uniqueness of player data and its subsequent use stems from two key differences. First, in virtual worlds, the nature of the non-IPI available to collectors is quite different. "Player data" might not be "personal" in the sense that it does not point to a specific physical individual, yet it continuously refers to a constant identity, and therefore can potentially provide its holders with meaningful insights. As users spend a great amount of time in a monitored environment, the electronic trail they leave behind may be of sufficient scope to allow game controllers to engage in effective and even unacceptable manipulative practices without requiring any personal information that pertains to the world outside the game. Second, in virtual worlds, the gaming companies' initiatives may lead to a unique problematic result — an undesirable addiction. Although virtual games are an enjoyable and even important experience for the majority of players, for others participation in virtual games can potentially become a form of addictive behavior

77. Clearly carrying out these schemes is problematic in view of the fact that other players might be aggravated in the event specific players are treated more favorably. The challenge for the game controllers will be finding ways to lure specific players back to the game without upsetting or even informing other players.

78. For examples as to how these practices are currently carried out in virtual worlds, see David Kennerly, Better Game Design through Data Mining, GAMASUTRA, Aug. 15, 2003, *at* http://www.gamasutra.com/features/20030815/kennerly_01.shtml.

79. For an in-depth analysis of the introduction of these practices through the use of data mining, see MYOB, *supra* note 10, at 6-17.

that resembles substance abuse or compulsive rituals.[80] Much has been said of the addictive attributes of the Internet's use in general; more specifically, chat rooms and other social networks facilitated by the online community. Virtual worlds, however, provide an additional level of seductiveness and potential for addictive behavior.[81] Recent research and anecdotal evidence[82] describe users who play for extensive periods of time, neglect their physical world duties and bodies, while causing grief and damage to themselves and others. Psychologists explain that this phenomenon results from a game's appealing digital interface, and the ability to receive immediate feedback and satisfaction when interacting in an MMORPG.[83]

The combination of these two aspects of virtual worlds (the richness of non-IPI and the danger of addiction) leads to a unique privacy concern: that game controllers can analyze and use non-IPI to motivate and influence players into engaging in excessive playing and, in extreme cases, encourage addictive behavior. Clearly, this fear does not pertain to all players. Yet for some, the availability and use of player data by gaming companies might lead to devastating results. In view of these possible outcomes, regulators must pay close attention to the means game controllers use to collect and manipulate "player data" to encourage negative and unhealthy addictions, especially among young people.

These potentially negative outcomes of player data analysis should not lead to overall restrictions of the collection and use of such information. The concerns mentioned could be addressed by

80. On the issues of the addictive nature of online virtual games, see Nick Yee, *Ariadne – Understanding MMORPG Addiction* (2002), at http://www.nickyee.com/hub/addiction/addiction.pdf (addressing the specifics of this addiction, and describes players that lose sleep, play for over ten consecutive hours, and other addictive behaviors). *See also* Brian Ng, *Addiction to Massively Multiplayer Online Role-Playing Games* (abstract) (Nov. 9, 2002), *at* http://faceweb.cti.depaul.edu/ctiphd/ctirs02/online_proceedings/Ng.htm.

81. *Cf.* Dr. Maressa Orzack, Computer Addiction Services, *at* www.computeraddiction.com (last visited Sept. 14, 2004) (asserting that virtual addiction is just another form of computer addiction).

82. For stories of the so-called "Ultima Widows," (i.e., relationships ruined in view of such addictions), see Julia Scheeres, *The Quest to End Game Addiction*, WIRED NEWS, Dec. 5, 2001, *at* http://www.wired.com/news/print/0,1294,48479,00.html.

83. *See* Yee, *supra* note 80. For a recent discussion regarding this issue and the psychology discourse in the "Terranova blog," see http://terranova.blogs.com/terra_nova/2004/06/onlinevideogame.html.

policies requiring gaming companies to assume some responsibility for the addictive behavior of vulnerable players, and act to mitigate, rather than potentially exacerbate these problematic behaviors. In this context, several policies and solutions implemented to assist compulsive gamblers in their interactions with casinos and other gambling facilities might be suited for the problems of addiction in virtual worlds.[84] For instance, gaming companies should consider introducing features that allow users to restrict unilaterally their playing time by setting a ceiling for the hours they could engage in playing during every day, week, or month. Moreover, game controls can apply their databases of "player data" to identify patterns of addictive conduct, alert players that may have a current or potential problem (while using the predictive models they have constructed), and suggest that they make use of these self-help measures. Such schemes would provide an example of the beneficial uses stemming from the collection and analysis of personal information — which demonstrates a solution that does not require the blocking of data collection.[85]

b. Increasing revenue by introducing additional services into virtual worlds

At this time, new business strategies to increase revenues in virtual worlds are already in the works, as game controllers strive to capitalize on their ongoing and extensive access to a large audience they "know" quite well. To meet this objective, several models are emerging (and will continue to emerge) for ways of using gaming space to promote advertising and marketing objectives. In a way, these models resemble similar practices implemented in other forms of media (including the Internet) where those controlling

84. For a description of self exclusion programs set in place as a protection from problem gambling (with extensive details as to the Missouri regulatory model and its success), see Kurt Eggert, *Lashed to the Mast and Crying for Help: How Self-Limitation of Autonomy Can Protect Elders from Predatory Lending*, 36 LOY. L. REV. 693, 748 (2003). *See also id.* at 754, for a discussion as to the implications of these programs for personal autonomy. For additional information regarding these forms of self-help solutions to gambling problems, see The Internet Gambling Prohibition Act of 1999, S. REP. NO. 106-121 (1999).

85. *See* Zarsky, *supra* note 14, for an extensive analysis of various privacy solutions and the overall argument against solutions premised on the limitation of collection. R

the medium sell advertisers "space" or "time" to promote brands and provide consumer information.

Gaming companies, however, quickly acknowledged that establishing these new forms of advertising initiatives and revenue streams is easier said than done. Serious difficulties arise from the game operators' ongoing effort to balance these schemes with their important business objective of ensuring and promoting player immersion in their virtual world. When players enter a MMORPGs and engage in extensive play, they expect to immerse themselves in these virtual worlds without encountering distracting or unrelated objects and messages that will fracture the delicate illusion of their virtual world.[86] Game creators have a distinct interest in preserving the immersive experience and keeping players fully engaged and satisfied. An additional difficulty in integrating advertising into virtual worlds arises from the specific settings of MMORPGs. Many of these games are set in a fantasy or ancient world, in which references to contemporary brands and products will seem awkward and out of place. Therefore, MMORPGs have been slower than other media in implementing various marketing and advertising schemes. This void was somewhat filled by "sponsored" games that provide free playing time online, in exchange for exposure to specific products or services.[87]

Yet, the problems described are mere setbacks and will not stop entrepreneurs from attempting to capitalize on the "attention goldmine" virtual worlds command. The first to overcome the immersion barrier and incorporate advertising into game space are the virtual worlds closely resembling our "physical" reality,[88] such as "Sims" or "There."[89] In these worlds, advertisers are finding ways to promote their brands without interfering with the game's harmony

86. I thank the contributors to the Terra Nova blog for pointing out these important problems with my analysis. For theses comments and others, see http://terranova.blogs.com/terra_nova/2004/01/vws_data_mining.html.

87. *See, e.g.*, www.WildTangent.com for a list of such games. *See also* Pethokoukis, *supra* note 36, for a description of the games developed for Toyota.

88. For a general discussion of these forms of virtual worlds, see Lastowka & Hunter, *supra* note 1, at 28.

89. It should be mentioned that even though The "Sims Online" has generated much interest and hype, it is not of the leading virtual worlds and is performing below the anticipated level. It indeed seems as if players prefer worlds that do not resemble the offline reality. It is hard, however, to predict what tomorrow's trends will show. For

and the players' immersion. For instance, recent reports indicate deals "The Sims Online" operators reached with both McDonald's and Intel for incorporating and promoting their brand products within the "Sims" virtual worlds.[90] McDonald's, for instance, allows players to operate a virtual franchise within the "Sims Online" world, where the "consumption" of burgers increases the player's social standing.[91] Another possible business strategy to further the commercialization of game space includes the promotion and sale of products directly connected to the game, within the virtual world. Such products could be "virtual" (such as virtual accessories that could be used in the virtual world),[92] or physical (such as real world apparel and accessories with the "game" logo — or even physical manifestations of the products sold and created within the virtual world). For instance, There.com has formed alliances with Nike and Levi's; these brands are sold within the virtual world for the avatar's use.[93] When applying these and other commercial models, game controls will surely take advantage of their ability to "narrowcast" separately to every specific player through the use of this digital medium. In doing so, they will try to tailor the specific advertising or marketing interface for every user in accordance to their personal data, preferences, and attributes.[94]

---

a recent description of the ongoing discourse evident in this virtual world, see *Sex, Mob Hits: Sims Tests Virtual Morals*, CNN.COM, July 5, 2003.

90. *See* Pethokoukis, *supra* note 36. R

91. *See* Michael Sansone, *Video Games and Advertising: Graphic Parallels with Early Game and Ad Copy and its Integration into New Media*, *at* http://www.nwe.ufl.edu/~sansone/twitchell/ (last visited Oct. 7, 2004).

92. For example, There.com allows for the promotion and sale of virtual jeans and sneakers. *See* Press Release, Connecting Chicago, There, Inc. Launches New Online Getaway Where Consumers Chat, Play and Connect Easily With Friends (October 27, 2003), *at* http://www.chicagoima.org/pre/102703.asp.

93. For more on There.com, see Lastowka & Hunter, *supra* note 1, at 28.

94. Several startup companies have tried to establish the technology and business models to implement such strategies. One such company was Adaboy, Inc., which seems to have folded after the dot.com boom. According to their webpage (www.theadstop.com), this company suggests the use of ads that are integrated into the game, presented in 3-D and are specifically tailored for the user. Targeting is based on demographic research, as well as previous accounts of exposure to the ads. *See also* Pamela Parker, *Internet Firms Play Ad Games*, INTERNETNEWS.COM, Apr. 7, 2000, *at* http://www.internetnews.com/IAR/article.php/337141. More recently, a new company — Massive Incorporated Inc. — has raised substantial capital to pursue a similar venture. *See* www.massiveincorporated.com for additional information.

The integration of advertising and marketing initiatives into an environment that enables the tailoring of specific content for every user on the basis of their personal profile leads directly to several privacy concerns.[95] Below I examine two problems often addressed in the "general" online context: fears that personal information will be used to discriminate among users, and concerns that such information will be used to manipulate them into consuming specific products.[96] I demonstrate how these two practices could be carried out in the "general" online worlds, and why these practices are at times problematic. I then shift the analysis to "virtual worlds" while demonstrating how such practices could be carried out on the basis of "player data" alone, thus presenting a unique privacy concern.

i. Price discrimination in virtual worlds

The Internet's ability to facilitate the "narrowcasting" of promotions, sales, advertisements, and marketing information on the basis of previously collected data allows vendors and marketers to engage in price discrimination — or, in other words, to provide the same product (or one slightly modified) to different users, for different prices. As anecdotal evidence indicating these dynamics trickles in from the media,[97] fears of such pricing schemes generate concerns in both the public[98] and academia. The underlying reasons for such concerns vary in accordance to the specific factors used to facilitate the differentiation between consumers.[99] At first, it is the fear that problematic factors (such as race, nationality, or gender) would be used within this pricing model to discriminate

95. Balkin, *supra* note 26, argues that the more commercialized games become, the more they will be subject to regulatory intervention. *Id.* at 4. In this Essay, I provide one reason as to why this assertion is indeed true – in view of growing privacy concerns. **R**

96. *See* MYOB, *supra* note 10, at 21-42, for an in-depth analysis of these issues.

97. *See* Amazon.com Varies Prices of Identical Items For Test, WALL ST. J., Sept. 7, 2000, at B19; Paul Krugman, *Reckoning; What Price Fairness?*, N.Y. TIMES, Oct. 4, 2000, at A35. For a discussion of these maters in greater depth, see Robert M. Weiss & Ajay K. Mehrotra, *Online Dynamic Pricing: Efficiency, Equity and the Future of E-Commerce*, 6 VA. J.L. & TECH. 11 (2001).

98. *See Opinion Surveys, supra* note 9. **R**

99. For an additional discussion on these issues, see MYOB, *supra* note 10, at 24-32. *See also* Paul Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WISC. L. REV. 743, 757 (2000); Lawrence Lessig, CODE AND OTHER LAWS OF CYBERSPACE 154 (1999).

among users. This set of concerns is inappropriate to our current discussion of the virtual persona and the possible uses of "player data," which does not include indications as to the users "offline" attributes.[100] Yet beyond these "problematic factors," online vendors can use other personal attributes to discriminate. Online data collectors can derive consumer choices and preferences from data regarding the times the user interacts online, the websites viewed, the products purchased, and the time of sale. Using this data, online vendors and content providers can generate elaborate models (by making use of advanced data mining applications)[101] that will provide meaningful insights as to their users' future behavior and demand curve regarding specific products at specific times.

These enhanced capabilities to collect and analyze personal information enable online vendors to price products and services in ways that are detrimental to their users, and achieve an unfair advantage in these transactions.[102] For example, such information will allow online vendors to set a marked-up price (or refrain from providing a discount) to users whom they believe are in dire need of the product, or lack price sensitivity or elasticity at specific junctures. In other words, the Internet framework allows online vendors to potentially benefit from their users' ignorance and vulnerability. Even though this issue may seem to be one of consumer protection law, it should be viewed as a privacy matter as well, as the sellers' advantage in these transactions results directly from their collection and use of personal information, and the user's inability to understand the implications of the collection of such data (which, in many cases, they willingly volunteer).

100. These issues are at times resolved by direct regulation. For instance, in the EU, Article 8(1) of the European Directive of Data Protection (Directive 95/46/EU) specifically notes several categories of personal information that cannot be collected–including information regarding race, religion and union membership.

101. Generally, data mining tools can alert analysts to patterns of behavior derived from personal data without the analyst generating an initial hypothesis or query. *See* MYOB, *supra* note 10, at 6-17, for in depth explanation as to the use of data mining applications to generate non-hypothetical driven results.

102. It should be noted that framing an argument against the practices of price discrimination is a difficult task, as there are several counter claims that draw out the efficiencies of these forms of pricing. On these issues, see Jonathan Weinberg, *Hardware Based ID, Rights Management, and Trusted Systems*, 52 STAN. L. REV. 1251, 1275 (2000); William W. Fisher III, *Property and Contract on the Internet*, 73 CHI-KENT L. REV. 1203, 1239 (1998) (with regard to intellectual property goods).

To carry through these pricing schemes, online sellers must obtain a vast amount of personal information about every user. Yet, in today's online reality, it is quite difficult[103] for one entity to form an extensive database to support these pricing schemes, which leads online companies to merge non-IPI with IPI, collected both on and offline.[104] This requirement however, to aggregate identifiable and non-identifiable information diminishes when shifting to virtual worlds. As virtual worlds integrate various business models that involve the sale of products and services for "real" money (or in exchange for a virtual currency that could be transformed to "real world" currency through a secondary market)[105] dynamic pricing methods of price discrimination in these settings will follow. Yet unlike other online settings, game controllers can launch effective discrimination schemes by relying on player data alone without requiring external data sources. Such player data — that traces the actions of users throughout very extensive interactions in game space — will also portray the actual purchasing patterns of consistent personas, and will provide game controllers and their affiliates with sufficient insight to carry through these problematic schemes. Since these schemes are implemented within the virtual world, the game controller need not know the true identity of the user, yet can discriminate among "avatars" that might represent imaginary identities, but are nevertheless engaging in actual transactions that involve "real world" currency.

It should be noted that practicing price discrimination in virtual worlds may prove to be very difficult in view of negative consumer opinions, and the possibility of a secondary market among users that will undercut effective price discrimination schemes ("the arbitrage problem").[106] Clearly, additional analysis is required regarding these points and should be pursued as virtual worlds move toward commercialization and retail. In addition, fu-

103. *See supra* notes 31-33 and relevant text. **R**

104. For example, the actions of DoubleClick that intended to aggregate its databases with those of Axciom – a large offline data collector. For an in depth discussion of this issue, see Richard M. Smith, *Internet Privacy: Who Makes the Rules*, 4 YALE SYMP. L & TECH. 2 (2001).

105. *See generally* Castronova, *supra* note 1. The central marketplace for these virtual commodities is Ebay – Category 1654. *See also* www.gamingopenmarket.com (last visited Oct. 7, 2004).

106. *See* Jonathan Weinberg, *supra* note 102, at 1275. **R**

ture research should examine the actual detriments such practices might cause, and whether game controllers must be required to disclose the occurrences of such pricing schemes.

ii. Manipulation

Beyond the use of personal information to set retail prices, online content providers can apply player data to tailor the specific content users receive. This practice, which on its face may seem useful and beneficial to users and information providers alike, might lead to problematic results. Access to personal information about users can facilitate manipulative forms of communications and advertising that abuse a specific user's vulnerability, achieve an unfair advantage, and even undermine the user's autonomy.[107] These manipulative practices are only partially effective in today's online world, as the datasets website operators can collect online are somewhat limited. Therefore, online content providers can only gain partial insights into their users' preferences and state of mind, and are limited in their persuasion and manipulation abilities. Yet these abilities will improve with time, and the public and legal discussion as to the possible detriments of these forms of manipulation has only started. For instance, the practice of targeting advertisements in the Internet realm on the basis of previously recorded online traffic data has already drawn public and legal scrutiny. Such targeting is carried out by intermediaries that gather information regarding users' online activities and surfing habits (that are mostly considered as non-IPI), and use such data to match specific advertisements for every user. DoubleClick Inc., a leader in this field, has been subject to ongoing public scrutiny, several lawsuits, and was finally forced to sign a settlement agreement that restricted its actions.[108] The public uproar in opposing these targeting practices could be understood, in part, as a reaction to

107. *See* MYOB, *supra* note 10, at 34-42.

108. It should be noted, however, that concerns regarding the actions of DoubleClick stemmed not only from their use of non-IPI in matching, but from their efforts to merge non-IPI with other databases of IPI, which was collected by other firms in the offline world. It is difficult to predict whether DoubleClick's business practices would have attracted such scrutiny should they have resulted from the analysis of non-IPI alone, which as mentioned above is usually considered as less harmful and significant. For more on these issues, see Smith, *supra* note 104. R

sophisticated advertising tools that attempt to persuade, while relying on insights into the specific user's interests and preferences (as reflected in their surfing habits).

As virtual worlds move toward commercialization, tailored advertising and other forms of commercial customized content are sure to follow, which will eventually lead to the above-cited concerns of manipulation. In this context, the uniqueness of privacy concerns in virtual worlds again stems from the problematic outcomes that could arise from the "mere" use of non-IPI data (or "player data"). Game controllers can use the virtual world's infrastructure to collect information regarding the preferences of a constant identity over an extended period of time, as well as create effective feedback loops by tailoring the content they present to every user, and constantly amending their responses in view of the user's most recent actions and reactions. Even when such information and interactions are restricted to worlds that are virtual, and at times ancient and imaginary, it provides insights to the specific user's actual perception and preferences: insights as to what forms of messages catch the player's attention and are comprehended effectively, at what instances users are most receptive to different ideas, and which forms of persuasion have succeeded in the past and will prove valuable when attempting to persuade or possibly manipulate. In addition, as the commercialization of virtual worlds continues, the data collected within these realms will include information as to the specific commercial preferences of the "avatar." Game controllers might use these unique abilities of non-IPI collection to engage in manipulative practices that will prove more effective and harmful than those carried through in the general online context, on the basis of non-IPI alone. These practices will require us to reconsider the harms of tailored persuasive content, as well as the implications of the collection of non-IPI in general, and our overall lenient attitude towards its subsequent use.

There are several ways to address this potential problem. One option would limit the collection and use of "player data." Another would require game controllers to adopt norms of transparency and provide their users with insights as to whether and why specific forms of content are personally tailored to every specific user. I prefer the latter path, as it will still provide for the ongoing collec-

tion of "player data," while protecting the interests of the specific players. Clearly, however, this issue requires further discussion and research.

IV. Virtual Worlds and Solutions to the Troubles of Information Privacy

After addressing the uniqueness of privacy concerns, this Essay now examines whether virtual worlds present specific challenges when assessing the relevance and projected success of solutions to the problems of online privacy. Specifically, I address a popular solution paradigm to the troubles of online privacy — market based solutions through the use of self-regulation.[109] Market based solutions and self-regulation are the dominant trend in the U.S. legal approach to online information privacy concerns.[110] Even though Congress enacted several laws regulating specific information sectors, many consider market-based solutions as a sufficient response to privacy concerns in a variety of unregulated information markets. In general, market-based solutions envision a society where the ongoing interaction between consumers and vendors lead to a competitive market in which users are presented with various options that offer a range of privacy standards. When faced with several options, users select their websites of choice, while taking into account their own privacy preference, the services the websites provide, their terms of service (including price), and finally, their privacy practices. Eventually, market forces will establish the various equilibrium "prices" at which users evaluate their privacy preferences in comparison to other benefits and requirements.

The key element to the success of any market-based solution in the online privacy context is the website operator's proper presentation and enforcement of their respective privacy policies. Operators must clearly display such policies, while indicating the privacy

109. On self-regulation in general (and specifically in the media context) see Angela Campbell, *Self-Regulation and the Media*, 51 Fed. Comm. L. J. 711 (1999). Of the possible meanings of "self-regulation," in this Essay I am referring to its narrowest sense; that in a specific market, it is the industry rather than the state that sets the standards. *Id.* at 715.

110. While it is true that a great variety of specific laws exist in order to solve privacy concerns, this form of solution governs the overall business realm. *See* Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 Hous. L. Rev. 717, 730-31 (2001).

practices and standards by which they abide. Thereafter, the public (through private actions) and the Federal Trade Commission (which has been doing so with only mixed success) will enforce these policies.[111] In addition, self-regulatory schemes rely on trusted third parties (such as BBB Online or TrustE) to provide websites with "seals of approval" that are contingent on their privacy standards and actual practices.[112] The efforts of such third parties assist users in following up on the actions of these commercial websites and assuring that they uphold their respective policies.

The market-based solution faces powerful critiques, stating that it is doomed to failure, for (among others) the following reasons:[113]

1. Privacy policies are an inadequate tool to enforce privacy standards; users do not read or understand them (as they are at times cloaked in heavy legalise) nor have the attention resources to comprehend every policy they encounter. Additional critiques point to the fact that the FTC lacks the manpower to enforce privacy policies, and that "third party" trusties might not be trustworthy, as they receive their compensation from the very same websites they are supposedly monitoring,[114] and

2. The market solution for privacy will fail in view of the high costs users face, such as high switching costs between online vendors and high information costs associated with the understanding of how the personal information might be used in the future.[115]

Examining these two critiques of the "market-based solution" with respect to our virtual world analysis leads to an interesting and mixed result: Some of the specific traits of virtual worlds indicate

111. On the FTC's commitment to enforce privacy promises, see http://www.ftc.gov/privacy/privacyinitiatives/promises.html (last visited Oct. 7, 2004). *See also* SOLOVE & ROTENBERG, *supra* note 5, at 540. R

112. On the issue as to whether it is worthwhile for a company to retain such a "seal" and a description as to what such retention entails, see Jeremy Quittner, *Should You Pay for a Privacy Seal of Approval?*, BUSINESSWEEK ONLINE, Apr. 27, 1999, *at* http://www.businessweek.com/smallbiz/news/date/9904/f990427.htm

113. For a recent critique of market-based solution in the privacy context, see James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 63 (2003).

114. *See* Zarsky, *supra* note 14, at 23. For an in-depth analysis as to the effectiveness of third party "seals", see Ann Cavoukian & Malcolm Crompton, *Web Seals: A Review of Online Privacy Programs*, *at* http://www.privacy.gov.au/publications/seals.html#424 (last visited Oct. 7, 2004). R

115. *See* Zarsky, *supra* note 14, at 40-41. R

that "market-based solutions" have a better chance of success in this realm, while others lead to the opposite conclusion.

On the one hand, in virtual worlds, privacy policies are a more effective means of conveying information and enforcing privacy. Here, users can limit their interactions and attention to a limited number of service providers (game sites), as opposed to the general online context where users might encounter tens of different websites — and thus privacy policies — every month. Therefore, users benefit from having all interactions carried out within one virtual world and being subject to only one, overall agreement, as the "attention costs" of understanding the various provisions of privacy policies are considerably lower. With only one or two relevant policies to review, the user will have the time and attention resources to contemplate whether he or she finds their terms and privacy implications acceptable.

On the other hand, virtual worlds change the "privacy market dynamic" in ways that will cause some of the abovementioned concerns to exacerbate. For an open market to provide solutions to privacy concerns, a competitive environment is required in which users choose and decide on the basis of their privacy preferences, and in that way signals these preferences to other market participants. Yet virtual worlds present users with high switching costs that impede on such signaling. In other words, users that might consider switching between "games" — should their game's operator change its privacy policy in a way they find unacceptable — will be reluctant to do so.[116] Users have gone to many lengths to construct and maintain a virtual persona in a specific virtual realm, and will be reluctant to forfeit the prestige and "assets" they accumulated, as they cannot transfer their acquired wealth and reputation to other

116. Most EULA's reserve the company's right to amend the agreement at their discretion at any time. In addition, the users, at the risk of losing all their online assets, must accept such changes. For instance, the Sims Online EULA states as follows: "*Your continued use of the Service thirty (30) days after a revised Terms of Service is posted on EA Online will mean that you accept all such revisions. If you don't agree to the changes, or to any of the terms in this Terms of Service, your only remedy is not to use EA Online and to cancel any Account or services you have signed up for.*" Note that recently online vendors have been constantly amending their privacy notices as well. *See* Janis Mara, *Companies Alter Privacy Policies*, Jan. 2, 2004, at http://www.esecurityplanet.com/trends/article.php/3294471. Yet here, arguably, the users have the option to switch to another user at a lower cost.

worlds.[117] These realities create very high switching costs, and at times even lock-in effects,[118] and will deter switching in a response to changes in privacy policies (and on the basis of privacy preferences).[119]

An additional reason for the unsuitability of market solutions to privacy problems in virtual worlds concerns the overall number of players in the virtual world's market. An effective market-based solution to privacy concerns requires a sufficient number of participants both on the supply and demand sides of the equation. In this context, the "virtual world" market is very different from the "general" online world that presents relatively low entry costs for vendors and service providers. Yet the fixed costs for creating and maintaining a virtual game are extremely high, and therefore the number of leading MMORPGs products is subsequently low.[120] Thus, there is no guarantee that privacy-sensitive users will be provided with sufficient alternatives (namely, optional virtual worlds), and an open market will fail to produce a virtual world that maintains high privacy standards.

A. Market-Based Solutions and Public Opinion

Public opinion has always been a dominant force in the ongoing debate about privacy standards and concerns.[121] In view of the imbalance of power between individual users and information collectors, the role of public opinion is essential in assuring that companies abide by their privacy polices, and deterring business

117. As a response to these problems, new initiatives have emerged to facilitate the transfer of "assets" from one virtual world to another. It still remains to be seen whether these companies become successful. *See, e.g.*, PlayVault.com, *at* http://www.playvault.com (last modified Sept. 10, 2004).

118. For an analysis of the possibilities and dangers of "lock-ins" in the broader online context, see Mark Klock, *Unconscionability and Price Discrimination*, 69 TENN L. REV. 317, 364 (2002).

119. A possible solution to this problem might be introducing specific regulations to lower the switching costs between games — for instance by requiring competing game operators to recognize credits, "wealth" and reputation accumulated in other gaming realms. Such a requirement however will consist of a serious intrusion into the gaming companies business models and therefore must be backed by concrete evidence of possible harms. Another possible option could be the creation (by mandate or market forces) of several privacy layers within the game.

120. For an additional analysis of this point, see CASTRONOVA, *supra* note 1, at 9.

121. *See generally*, LAURA J. GURAK, PERSUASION AND PRIVACY IN CYBERSPACE (1997).

initiatives that raise privacy concerns. In terms of the previous analysis, an active public discourse about privacy concerns lowers the user's information costs that are associated with comprehending the future uses of their personal information. It also "signals" the individual's discomfort with or disapproval of various privacy practices in a manner that is more vocal than the voice of a single individual. The strength and importance of public opinion has been evident in the Internet context, as on several occasions Internet vendors and service providers changed their problematic privacy practices in view of "bad press" and threats of consumer retaliation.[122] The powerful force of "public opinion" in the online context results from the speed and efficiency in which news and information flow throughout the web, and consequently, facilitate the quick formation of resistance groups and communities. The social networks created online allow their members to easily contact each other (via an email list, a listserv, or a chat-room) and work together toward a common cause, even though the participants come from varied backgrounds and geographical locations.[123]

Establishing the difference between the forces of public opinion in virtual worlds as opposed to the general online context is a difficult task. Game activists and players will claim that the gaming environment provides unusual strength and weight for the user's opinion, citing the benefits of the game's social network environment (similarly to the arguments made in the online context, above). Furthermore, users are in a strategically superior position in virtual worlds, because the consumer (rather than the advertisers) is the major source of the game producer's income. Therefore, it seems reasonable to anticipate that game controllers will be attentive to their users' requests and complaints.

In virtual worlds, however, game controllers have a key advantage that might hinder the presumed strength of public opinion — the ability to silence opposing voices. They can achieve this objective by simply removing critical speakers from game space.[124] When

122. *See id.*

123. An extreme example is the creation of Linux and other open source and peer production projects. *See* Yochai Benkler, *Coase's Penguin, or, Linux and the Nature of the Firm*, 112 YALE L.J. 369, 381-400 (2002).

124. In one famous incident, Peter Ludlow, who runs the "Alphaville Herald" that described life in the Sims Online virtual time, was removed from the game. Though

removed from the virtual world, these "abolished speakers" will encounter severe difficulties in gathering support for antagonistic ideas, and will be forced to try and reach their audience through alternative means, such as web forums devoted to a specific game[125] (which is clearly a less effective way to communicate). Since the gaming worlds are "guarded" by code,[126] unwanted speakers will find it impossible to re-enter and voice their opinion. Furthermore, there are other, subtler ways for the game controllers to "silence" antagonists. As game controllers can closely view the ongoing interactions and discourse among the various users, they might attempt to obstruct the distribution of these antagonistic messages by tampering with the virtual world's infrastructure (by setting mountains between potential antagonists, or not allowing them to talk with more than one person at a time).

To summarize this brief analysis of the market-based and self-regulatory solutions to privacy concerns in virtual worlds, it appears that the success of any such scheme will depend on the ability of users to continuously and constantly interact, without the fear of censorship or abolishment by the game operators. The extent of privacy concerns and problems will be closely linked to further understanding the speech rights of players interacting within the game.[127] By maintaining a constant flow of information among players, society may avoid the privacy concerns illustrated above, without requiring the overall regulation of the game controllers' practices of collection and use of "player data." Specific interven-

Electronic Arts cited a technical breech of the EULA as the reason for such removal, Ludlow argues he was removed so to silence his provocative reporting. *See* Harmon, *supra* note 37.

125. For example, through game discussion boards, which exist in the thousands online. See reference to the Everquest boards at Lastowka & Hunter, *supra* note 1, at 59. As mentioned in this article, however, the power of voicing an opinion in such boards does not approach the discourse possible within the game.

126. Therefore, any unauthorized entrance will be subject to the harsh anti-hacking laws put in place to protect computer networks (such as the Computer Fraud and Abuse Act ("CFAA")). On anti-hacking laws, see generally, SOLOVE & ROTENBERG, *supra* note 5, at 503. R

127. *See* Balkin, *supra* note 26, at 34, for an analysis as to whether virtual worlds might constitute a public forum and therefore should be subject to stricter free speech requirements (which might in fact forbid the removal of opposing ideas). *See also* Lastowka & Hunter, *supra* note 1, at 60. R

tions however might still be required at the problematic junctures identified in Section II.

V. Conclusion

The analysis I provide in this Essay is only the beginning of a journey — one that I hope others will travel as well — and an attempt to draw out a roadmap for understanding the unique issues of information privacy in virtual games. These issues require additional research that must closely examine the ongoing changes both in the technology facilitating the virtual worlds, as well as the social and legal landscape that governs issues of information privacy in general, and online privacy in particular. I believe, however, this analysis sufficiently demonstrates the importance of a discussion of privacy rights in virtual worlds — both as an intriguing issue of its own merit, and as an important tool for sharpening our understanding of privacy concerns.