

6-2012

Avatar Experimentation: Human Subjects Research in Virtual Worlds

Joshua A.T. Fairfield

Washington & Lee University

Follow this and additional works at: <https://scholarship.law.uci.edu/ucilr>

 Part of the [Contracts Commons](#), [Intellectual Property Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

Joshua A. Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, 2 U.C. IRVINE L. REV. 695 (2012).

Available at: <https://scholarship.law.uci.edu/ucilr/vol2/iss2/10>

This Article is brought to you for free and open access by UCI Law Scholarly Commons. It has been accepted for inclusion in UC Irvine Law Review by an authorized editor of UCI Law Scholarly Commons.

Avatar Experimentation: Human Subjects Research in Virtual Worlds

Joshua A.T. Fairfield*

Researchers love virtual worlds. They are drawn to virtual worlds because of the opportunity to study real populations and real behavior in shared simulated environments. The growing number of virtual worlds and population growth within virtual worlds has led to a sizeable increase in the number of human subjects experiments taking place in such worlds.

Virtual world users care deeply about their avatars, their virtual property, their privacy, their relationships, their community, and their accounts. People within virtual worlds act much as they would in the physical world because the experience of the virtual world is “real” to them. The very characteristics that make virtual worlds attractive to researchers complicate ethical and lawful research design. The same principles govern research in virtual worlds and the physical world. However, the change in context can cause researchers to lose sight of the fact that virtual world research subjects may suffer very real harm to property, reputation, or community as the result of flawed experimental design. Virtual world research methodologies that fail to consider the validity of users’ experiences risk harm to research subjects. This Article argues that researchers who put subjects’ interests in danger run the risk of violating basic human subjects research principles.

Although hundreds of articles and studies examine virtual worlds, none have addressed the interplay between the law and best practices of human subjects research in those worlds. This Article fills that gap.

Virtual worlds are valuable research environments precisely because the relationships and responses of users are measurably real. This Article concludes that human subjects researchers must protect the very real interests of virtual worlds inhabitants in their property, community, privacy, and reputations.

This Article proceeds in five parts. After Part I introduces the scope of the piece, Part II explains virtual worlds and discusses why the

* Associate Professor of Law, Washington & Lee University School of Law, and Director, Frances Lewis Law Center. Many thanks to my research assistants, Kelley Bodell, Angela Merley, and Michael Bombace, for their invaluable help in completing this piece.

marriage of social networking with three-dimensional videogame graphics complicates experimental design. Part III explores current and developing practices in virtual worlds research, as well as the various areas of law that bear on such research. Part IV outlines solutions and best practices for human subjects research in virtual worlds, and Part V offers a conclusion.

I. Introduction	697
II. Virtual Worlds	698
III. Human Subjects Research: Practice and Law.....	702
A. Practice	703
1. Primary and Secondary Research	704
2. Qualitative Research Methodologies	705
3. Quantitative Research Methodologies.....	707
B. Law	709
1. The Belmont Report and Federal Common Rule.....	709
a. Autonomy.....	720
b. Beneficence.....	725
c. Justice	728
d. Special Protections for Minors in Virtual Worlds	730
e. The Advance Notice of Proposed Rulemaking (ANPRM)	732
2. Copyright and Terms of Service/End User License Agreement	737
a. Copyright in Virtual Worlds.....	737
b. Defenses to Copyright Infringement	740
c. Implications of Copyright and Licensing Law for Virtual Worlds Research Tools.....	743
3. Privacy Law	750
a. Privacy Torts	750
b. Statutory Privacy Regimes	755
IV. Best Practices	762
A. Exclusion or Redaction of Private Messages	762
B. Exclusion of Minors	763
C. Obtaining Adequate Informed Consent	764
1. Primary Research	764
2. Secondary Research	765
D. Respecting In-World Cultural Norms	766
E. Treatment of Avatar Names as Identifiable Private Information or Personally Identifiable Information	767
F. Anonymization of Personally Identifiable Information for International Transport.....	769
G. Diversifying the Research Pool of Virtual Worlds	770
H. Educating and Working With IRBs	770
I. Using Add-Ons and Scrapers Effectively and Appropriately.....	771
V. Conclusion	771

I. INTRODUCTION

Researchers love virtual worlds. They have been drawn to virtual worlds because of the unprecedented opportunities such environments offer for the detailed study of large and complicated social groups within a shared virtual context. Virtual environments offer a far greater range of experimental possibilities than the physical world can provide. The growth in numbers of and participation in virtual worlds has therefore driven a significant increase in the number of virtual world human subjects experiments.¹ The data collected in these virtual world studies describe real human responses to situations that the users experience as real, even though the experiments are conducted in virtual spaces.²

Yet experiments in virtual worlds are very difficult to conduct ethically and lawfully. Virtual world users care deeply about their avatars, their virtual property, their privacy, their reputations, their relationships, their community, and their accounts. Although no ethical researcher would knowingly harm subjects' property or reputational interests, some common research methodologies risk harming those interests as they appear in virtual worlds. Researchers who put these interests at risk may unknowingly violate basic principles of human subjects research.

Of the hundreds of articles about virtual worlds, none have examined in depth the law that governs virtual worlds research.³ This Article fills that gap. The Article's core argument is that virtual world researchers must recognize their

1. See Nate Anderson, *Sociologists Invade World of Warcraft*, See *Humanity's Future*, ARS TECHNICA (May 9, 2010, 10:00 PM), <http://arstechnica.com/search> (search "sociologists invade world of warcraft" and follow the link of the same title) ("While playing *World of Warcraft* and traipsing through *Second Life* might not sound like traditional academic disciplines, they are increasingly important for research into virtual communities.").

2. See Tyler Pace et al., *The Rogue in the Lovely Black Dress: Intimacy in World of Warcraft*, 28 CONF. HUM. FACTORS COMPUTING SYS. 233, 235 (2010) ("At the basis of all our findings is a rejection of the commonly held dichotomy that radically separates the real world from a virtual one . . . Without a doubt, real world mental models of intimacy shape the perception and construction of virtual intimacy."). Note here that researchers can fail to internalize the risk users take when participating in virtual worlds research even if they are sensitive to the connections between real and virtual worlds. Researchers must do more than acknowledge the "realness" of virtual world interactions; they must proactively design methodologies that safeguard research subjects' virtual communities.

3. A sample, rather than a survey, of this rapidly growing field would include: Jack M. Balkin, *Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds*, 90 VA. L. REV. 2043 (2004); Michael A. Carrier & Greg Lastowka, *Against Cyberproperty*, 22 BERKELEY TECH. L.J. 1485 (2007); Edward Castronova, *The Right to Play*, 49 N.Y.L. SCH. L. REV. 185 (2004); Joshua A.T. Fairfield, *Virtual Property*, 85 B.U. L. REV. 1047 (2005); Dan Hunter, *Walled Gardens*, 62 WASH. & LEE L. REV. 607 (2005); F. Gregory Lastowka & Dan Hunter, *The Laws of the Virtual Worlds*, 92 CALIF. L. REV. 1 (2004); Leandra Lederman, "Stranger than Fiction": Taxing Virtual Worlds, 82 N.Y.U. L. Rev. 1620 (2007); Juliet M. Moringiello, *What Virtual Worlds Can Do for Property Law*, 62 FLA. L. REV. 159 (2010); Erez Reuveni, *On Virtual Worlds: Copyright and Contract Law at the Dawn of the Virtual Age*, 82 IND. L.J. 261 (2007); Dmitri Williams et al., *Who Plays, How Much, and Why? Debunking the Stereotypical Gamer Profile*, 13 J. COMPUTER-MEDIATED COMMUN 993 (2008); Robin Fretwell Wilson, *Sex Play in Virtual Worlds*, 66 WASH. & LEE L. REV. 1127 (2009).

subjects' very real interests in property, reputation, community, and privacy. Part II therefore explains virtual worlds and discusses why virtual worlds technology—especially the growing link between virtual worlds and the real world—complicates experimental design. Part III explores current and developing practices in virtual worlds research, as well as various areas of law that bear on such research. Part IV outlines solutions and best practices for human subjects research in virtual worlds, and Part V offers a conclusion.

II. VIRTUAL WORLDS

Virtual worlds are often described as avatar-mediated, pseudophysical, social, persistent, synchronous, and interactive shared spaces.⁴ Avatars are users' carefully crafted virtual representations within the shared online space.⁵ That space is pseudophysical, referring to the sense of place and context users experience in a virtual world.⁶ Shared spaces populated by avatars are used for social purposes—the entire purpose of the space is to share it with other users, who are themselves represented by avatars.⁷ Persistence indicates that the world remains when any given player is offline.⁸ The world is not entirely dependent on the player as would be three-dimensional spaces created for a single multiplayer game of Halo, for example.⁹ Interactivity builds on persistence because the actions of one player in the world can impact the shared environment, and thus the experience of all the other players.¹⁰ Synchronicity is a temporal characteristic: it means that players generally are required to be logged in at the same time in order to interact with

4. See Edward Castronova, *Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier* 5–6 (CESifo, Working Paper No. 618, 2001), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=294828 (defining virtual worlds in terms of “interactivity,” “physicality,” and “persistence”); F. Gregory Lastowka & Dan Hunter, *Virtual Worlds: A Primer, in THE STATE OF PLAY: LAW, GAMES, AND VIRTUAL WORLDS* 13, 15 (Jack M. Balkin & Beth Simone Noveck eds., 2006).

5. See Jonathon W. Penney, *Privacy and the New Virtualism*, 10 YALE J.L. & TECH. 194, 221 (2008) (describing an avatar as “a visible representation of [the user’s] persona in the virtual world”). Penney goes on to explain: “People can define their avatar as they wish, similar to or completely different from their actual physical appearance. The avatar is a 3D character that is completely controlled by the member; the avatar *is* the person in the virtual world.” *Id.*

6. See Castronova, *supra* note 4, at 6 (“[P]eople access the program through an interface that simulates a first-person physical environment on their computer screen . . .”).

7. See *id.* (“[T]he environment is generally ruled by the natural laws of Earth and is characterized by a scarcity of resources.”).

8. See Lastowka & Hunter, *supra* note 4, at 15 (describing persistent worlds as those where “the environment continues to exist and changes over time,” despite a given player logging off).

9. In Halo, environments are generated in one-off multiplayer matches; once the players are finished with the match and leave the game, the environment disappears. The next match takes place in a newly generated environment.

10. See Lastowka & Hunter, *supra* note 4, at 6 (providing examples of interactivity like “your neighbors’ virtual houses [being] remodeled and redecorated while you commute to work”).

one another.¹¹ Virtual worlds like World of Warcraft and Second Life are embodiments of this traditional virtual world definition.¹²

Yet virtual worlds are rapidly changing. Virtual worlds are now a sufficiently mainstream phenomenon for their definition to include some diversity of opinion.¹³ I have in prior work described virtual worlds by reference to the technological trends that generated them: the advances in video game graphical user interface married to rapidly evolving and expanding social networking applications.¹⁴ This definition expands the field and includes many new, exciting, and rapidly growing environments.

For example, my definition would include Farmville,¹⁵ Zynga Game Network's popular Facebook application, while the traditional definition of virtual worlds would likely exclude it. The Farmville interface uses low-grade isometric animation, is not truly synchronous, and is, in fact, surrounded by the usual Facebook borders linking the player's real-world identity to the game.¹⁶ Farmville is an example of how synchronicity and pseudophysicality become less important as connections to the users' real world identities become more prevalent. Real-world associations provide an important part of the context shared by the users.

The new definition also serves to highlight the tension between the graphical and social elements of virtual worlds. The better the game graphics of a virtual world, the fewer people have the computers or the bandwidth necessary to use the world. As game graphics increase in clarity and complexity, the pool of potential users shrinks. Virtual world developers—called “game gods” in technology parlance—seek a sweet spot, where the graphics are good enough to induce the emotional and economic reactions for which virtual worlds are so rightly famous, while keeping the costs (in gear and bandwidth) of access from becoming prohibitive. This tension has been resolved increasingly in favor of the social over the graphical. As virtual worlds have gone mainstream, they have used simpler

11. See Castronova, *supra* note 4, at 6 (noting that when worlds are accessed “simultaneously by a large number of people . . . the command inputs of one person affect[] the command results of other people”).

12. See Peter J. Quinn, *A Click Too Far: The Difficulty in Using Adhesive American Law License Agreements to Govern Global Virtual Worlds*, 27 WIS. INT'L L.J. 757, 766 (2010) (“[B]oth *Second Life* and *World of Warcraft* have significant popular culture footprints and thus essentially define the current iteration of virtual worlds.”).

13. The frequent mention of virtual worlds in the popular news is evidence of their presence in the mainstream. See, e.g., Alexandra Alter, *My Virtual Summer Job*, WALL ST. J., May 16, 2008, at W1; Shira Boss, *Even in a Virtual World, ‘Stuff’ Matters*, N.Y. TIMES, Sept. 9, 2007, at B1; Sara Corbett, *Portrait of an Avatar*, N.Y. TIMES MAG., Mar. 8, 2009, at 22; Katie Hafner, *At Sundance, a Second Life Sweatshop Is Art*, N.Y. TIMES, Jan. 28, 2008, at C5; Robert O’Harrow Jr., *Spies’ Battleground Turns Virtual: Intelligence Officials See 3-D Online Worlds as Havens for Criminals*, WASH. POST, Feb. 6, 2008, at D1.

14. See Joshua A.T. Fairfield, *The God Paradox*, 89 B.U. L. REV. 1017, 1019 (2009).

15. See FARMVILLE, <http://www.facebook.com/farmville> (last visited June 6, 2012).

16. *Id.*

interfaces and graphics to attract a broader audience.¹⁷ Virtual worlds are gravitating toward the virtualization of social networking environments (e.g., Farmville) instead of the three-dimensional, immersive, and graphical ideal represented in the movie *The Matrix*.

Virtual worlds are also mirroring social networks in that their primary methods of communication are becoming asynchronous and tied to real-world identity. Virtual worlds have always incorporated in-world electronic messaging systems (e-mails and instant messages (IMs)), and have now developed methods for integrating the virtual world with outside communications. For example, there are iPhone apps for the World of Warcraft auction house system that permit traders to continue their virtual economic activity while logged off.¹⁸ Most virtual worlds provide some form of external connection to e-mail. Thus, if you receive an instant message in Second Life, you can also receive an e-mail.¹⁹ The synchronicity element is also under assault from the other direction. Traditionally asynchronous methods of communication are becoming more and more synchronous. For example, mobile phone technologies now integrate push e-mail.²⁰ Other asynchronous platforms, such as Facebook and Twitter, continue to evolve into near-real-time connections.²¹ Thus, synchronicity plays less of a role in new virtual environments than does asynchronous or near-synchronous communication.

This Article embraces the social-networking and community nature of virtual worlds. Virtual world technologies are seeping out of sword-and-sorcery games and into social networks,²² as well as out of computers and onto mobile devices.²³ The definition of a virtual world is necessarily evolving as elements of virtual worlds begin to appear in increasingly mainstream social networks and on new

17. *Compare Realm Stats*, WARCRAFT REALMS, <http://www.warcraftrealms.com/realmstats.php> (last visited June 6, 2012) (listing usage statistics), *with Application Metrics*, APPDATA, <http://www.appdata.com/apps/facebook/102452128776-farmville> (last visited June 6, 2012) (listing usage statistics).

18. *World of Warcraft Remote*, BLIZZARD, <http://us.battle.net/wow/en/services/wow-remote> (last visited June 6, 2012).

19. *See Instant Messages*, SECOND LIFE, <http://community.secondlife.com> (last visited June 6, 2012) (describing the preference option to forward IMs to e-mail for offline notifications).

20. Push e-mail refers to when a user's e-mail is pushed from a server to the user's phone automatically and instantly, instead of the user's phone pulling the e-mail from the server at assigned intervals. *See Definition of Push E-mail*, PCMAG, http://www.pcmag.com/encyclopedia_term/0,2542,t=push+e-mail&i=49975,00.asp (last visited June 6, 2012).

21. *See United States v. Fumo*, 655 F.3d 288, 331 (3d Cir. 2011) ("The Internet, especially social networking sites like Facebook and Twitter, have created a society that is 'connected' at all times.").

22. *See FARMVILLE*, *supra* note 15.

23. *See, e.g., PARALLEL KINGDOM*, <http://www.parallelkingdom.com> (last visited June 6, 2012) (virtual world overlaid on top of the real world and played over geolocated smartphones); *Pocket Empires Online: The Ultimate MMO War Game on Android*, ANDROID & ME (Apr. 3, 2011, 4:17 PM), <http://androidandme.com/2010/04/games/pocket-empires-online-the-ultimate-mmo-war-game-on-android> (describing Pocket Empires, a mobile virtual world).

forms of handheld devices. With this new approach, it is possible to extend the definition of a virtual world to cover new trends without sacrificing clarity.

The concerns and solutions raised by this Article thus have a broad application. While traditional virtual worlds are grounded in sword-and-sorcery fantasy, social networks are about real life. Social networks connect actual identities, interests, and relationships. The gap between social networks and virtual worlds is diminishing. As the gap disappears, virtual world research methodologies must adapt. Avatars are ever more personally identifiable; property, community, privacy, and reputation in virtual worlds are becoming indistinguishable from property, community, privacy, and reputation in real life. Harm to the virtual aspects of a person is becoming functionally indistinguishable from harm to the real-world aspects of that person.

The increasingly porous boundary between the real world and virtual worlds speaks to the core claim of this Article: virtual worlds researchers may unwittingly harm users' virtual items, objects, accounts, avatars, and communities because they do not fully account for the quite real nature of these assets. An avatar, for example, does not merely represent a collection of pixels—it represents the identity of the user. The user is known by the avatar's name and is represented in the virtual world by the avatar.²⁴ The avatar is the connection of the user to the online social community. Likewise, virtual reputations and trust are costly to generate but easy to lose.²⁵ If an avatar is identified as having harmed the community through interactions with a researcher, the human being behind the avatar will certainly suffer harm to identity, reputation, and community.

In the same vein, the accumulation of property in virtual worlds often reflects very real economic interests of the human subject.²⁶ Many virtual worlds have in-world economies.²⁷ These virtual economies have grown rapidly and have

24. See Penney, *supra* note 5.

25. See Jeffrey Aresty, *Digital Identity and the Lawyer's Role in Furthering Trusted Online Communities*, 38 U. TOL. L. REV. 137, 140 (2006) ("Creating trust between two parties interacting in the virtual world is more difficult to accomplish than it is in real life.").

26. See Complaint at 5, *Eros v. Linden Research, Inc.*, No. 09-04269 (N.D. Cal. dismissed March 16, 2011) ("The ability to exchange Linden Dollars for U.S. Dollars—combined with Linden Lab's encouragement and development tools—has allowed true commercial activities to flourish within Second life, with user-to-user transactions surpassing 120 million (U.S.) in the First Quarter of 2009 alone.").

27. See Joey Seiler, *What Can Virtual-World Economies Tell Us About Real-World Economies?*, SCI. AM. (Mar. 17, 2008), <http://www.scientificamerican.com/article.cfm?id=virtual-world-economists-on-real-economies> (listing virtual worlds that facilitate burgeoning economies, including EVE Online, Second Life, and Entropia Universe). See also Linden Research, *LindeX Exchange: Market Data, SECOND LIFE*, http://community.secondlife.com/t5/English-Knowledge-Base/Buying-and-selling-Linden-dollars/ta-p/700107#Section_1 (last visited June 6, 2012) (explaining how to exchange U.S. dollars for Second Life currency).

begun interacting with the real-world economy.²⁸ People now routinely use real dollars to purchase virtual land, goods, and services.²⁹

This meshing of virtual and real-world economies was at first unintended, and often resisted, by the virtual worlds developers.³⁰ However, numerous online environments, including prominent social networks, are now exploring the sale of virtual objects and currencies as a microtransactions business model.³¹ If a research methodology causes the game god to ban a subject's account, the subject can lose real reputation, real community, and real money. Reputation, community, and money in the offline world may be more widely recognized than the same social constructs in virtual worlds, *but they are all equally real*. The loss of these social constructs, whether real or virtual, harms the human subject. This is precisely the sort of harm that human subjects research law seeks to prevent.

III. HUMAN SUBJECTS RESEARCH: PRACTICE AND LAW

Researchers must first ensure that their research designs comport with commonly accepted ethical research standards.³² Because virtual worlds research is nascent, researchers often struggle to adapt established methods to virtual world contexts. The first subpart below analyzes the challenges raised by attempts to develop ethical research methodologies for use in virtual worlds.

Second, researchers will wish to abide by the law of the land in which they conduct research, and research in virtual worlds is no exception. Although researchers may conceive of virtual worlds as free from real-world legal jurisdiction, this is far from true. Diverse areas of law, including federal research funding regulations, copyright, privacy torts, statutory privacy regimes, criminal

28. See *The New New Economy: Real Money in a Virtual World*, KNOWLEDGE AT WHARTON, <http://www.knowledgeatwharton.com.cn/index.cfm?fa=printArticle&articleID=1261&languageid=1> (last visited June 6, 2012) ("This virtual wealth was innocuous until people began paying real greenbacks for it on eBay or any number of trading sites.").

29. See Judith A. Powell & Lauren Sullins Ralls, *Best Practices for Internet Marketing and Advertising*, 29 FRANCHISE L.J. 231, 236 (2010) ("Real money changes hands in [Second Life] through the buying and selling of virtual goods and services—a staggering \$35 million a month.").

30. See Daniel Terdiman, *Sony Scores with Station Exchange*, CNET NEWS (Aug. 25, 2005, 4:00 AM), http://news.cnet.com/Sony-scores-with-Station-Exchange/2100-1043_3-5842791.html?tag=mncol;txt ("Until Sony launched the Station Exchange on July 19 [2005], however, almost all secondary market trading—though common—was officially banned by nearly all publishers of MMOs in their terms of service or end-user license agreements.").

31. See Alex Pham, *Facebook and Zynga Game Network Reach Five-Year Deal*, L.A. TIMES, May 19, 2010, available at <http://articles.latimes.com/2010/may/19/business/la-fi-facebook-20100519> (describing an agreement whereby Zynga and potentially all Facebook developers use Facebook credits, a platform-wide virtual currency bought with real-world currency, for all online commerce); see also Mark Wallace, *The Game Is Virtual. The Profit Is Real*, N.Y. TIMES, May 29, 2005, at 7, <http://www.nytimes.com/2005/05/29/business/yourmoney/29game.html> (describing one user's Second Life business earning real profit of approximately \$1,800 per month).

32. This includes, among other things, passing an institutional review board (IRB) review that checks for conformity with federal human subjects research standards. See discussion *infra* Part III.B.1 (describing the IRB review process).

laws, and even foreign laws and international agreements all govern virtual worlds. The second subpart below will discuss these areas and the challenges they pose to virtual worlds researchers.

Some concrete examples may serve to clarify the challenges that researchers face in virtual worlds. Players in virtual worlds send text to each other in both private and public chat. Researchers must consider, based on law and established ethical practice, whether capturing and parsing private chat is a violation of the users' expectations of privacy. Another issue: human subjects must give consent before being subjected to research. Researchers must determine whether the kind of consent involved in online consumer End User License Agreements (EULAs) is sufficient to meet the standards of informed consent to human subjects experimentation. A third example: researchers routinely record their subjects and their environments in realspace research. But in virtual worlds, avatars and environments are subject to numerous copyrights, often owned by different people, all of which must be properly licensed before recording. For all of these challenges and more, researchers must make the best adaptation possible of existing research practices and attempt to map those practices onto an alien and rapidly shifting legal landscape.

A. Practice

Internet research ethicists Heidi McKee and James Porter note: "Although there has been considerable discussion on Internet research ethics generally over the past ten years, there has not as yet been much published research on the distinctive ethical challenges of conducting research in MMOGs [massively multiplayer online games] and virtual worlds."³³ The following subparts discuss primary and secondary research, as well as qualitative and quantitative research methods, both as they are used offline and as adapted to virtual worlds.³⁴ The emphasis is not on the comparative effectiveness of such methods, but on attributes of research methodologies most likely to implicate legal issues.³⁵

33. HEIDI A. MCKEE & JAMES E. PORTER, THE ETHICS OF INTERNET RESEARCH: A RHETORICAL, CASE-BASED PROCESS 114 (2009); see also, e.g., Charles Ess et al., *Ethical Decision-Making and Internet Research* (2002) (Association of Internet Researchers Ethics Working Committee recommendations), available at <http://aoir.org/reports/ethics.pdf> (last visited June 6, 2012); Mark S. Frankel & Sanyin Siang, *Ethical and Legal Aspects of Human Subjects Research on the Internet* (Nov. 1999), available at <http://www.aaas.org/spp/sfhl/projects/intres/report.pdf> (report of U.S. Office for Protection from Research Risks (now OHRP) sponsored workshop on Internet ethics).

34. Of course, few experiments use only one methodology. Often researchers make use of mixed methods, which incorporate elements of both methodologies. See generally John W. Creswell, *Editorial: Mapping the Field of Mixed Methods Research*, 3 J. MIXED METHODS RES. 95 (2009).

35. A discussion of the comparative merits of qualitative and quantitative research is beyond the scope of this Article, as is a comparison of the various quantitative methods. Thus, for example, the question of whether machine-learning algorithms sufficiently demonstrate causation is a lively debate. Machine-learning algorithms are certainly commonly used in the analysis of virtual world

1. *Primary and Secondary Research*

In primary research, the researcher directly obtains information from the subject through observation, interview, survey, or any other method.³⁶ In secondary research, the researcher obtains and parses a data set gathered by someone else, whether another researcher or a commercial entity.³⁷

Commercial databases are increasingly relevant to virtual worlds research. Game gods license enormous collections of data to researchers for secondary analysis.³⁸ These databases are comprehensive repositories of nearly every action taken and word spoken in a virtual world.³⁹ The game gods gather this

data. However, this question is one for social scientists, not lawyers. I do not here analyze the potential inaccuracies caused by use of any given research method.

36. See, e.g., Dana Lynn Driscoll & Allen Brizee, *What Is Primary Research and How Do I Get Started?*, OWL (Apr. 17, 2010), <http://owl.english.purdue.edu/owl/resource/559/01> (“Primary research is any type of research that you go out and collect yourself.”).

37. See Kenneth D. Bailey, *Quantitative Methodology*, in 21ST CENTURY SOCIOLOGY 108, 110 (Clifton D. Bryant & Dennis L. Peck eds., 2007) (describing the data collection methods of secondary researchers).

38. See, e.g., James Brightman, Nielsen, *EEDAR Team Up for Video Game Data Service*, INDUSTRY GAMERS, (Nov. 2, 2009) <http://www.industrygamers.com/news/niesen-cedar-team-up-for-video-game-data-service> (describing the combination of EEDAR and Nielsen data to create a more comprehensive database of user activity); *GamePulse*, EEDAR, <http://www.eedar.com/Services/GamePulse.aspx?p=9> (last visited June 6, 2012) (“With information on every console game product released since 2000, PC since 2006 . . . GamePulse keeps abreast of the entire landscape of the video game industry . . . EEDAR continues to work with publishers and research providers to integrate new data sets as they become viable.”); Chris Lewis & Noah Wardrip-Fruin, *Mining Game Statistics from Web Services: A World of Warcraft Armory Case Study*, FDG ‘10: PROCEEDINGS OF THE FIFTH INT’L CONF. ON THE FOUND. OF DIGITAL GAMES 1 (2010), available at <http://games.soe.uesc.edu/sites/default/files/wowspyder.pdf> (describing the research utility of a web crawler program that indexes and downloads information from web services like World of Warcraft Armory); Brian Tarran, *Nielsen Scores Game Data Deal with Sony*, RESEARCH MAG. (July 2, 2007) <http://www.research-live.com/news/nielsen-scores-game-data-deal-with-sony/3003365.article> (describing Sony’s data as part of the data set that would comprise Nielsen’s “monthly reports of audience stats and user activity . . .”); John Timmer, *Science Gleans 60TB of Behavior Data from Everquest 2 Logs*, ARS TECHNICA (Feb. 15, 2009, 4:00 PM), <http://arstechnica.com/science/news/2009/02/aaas-60tb-of-behavioral-data-the-everquest-2-server-logs.ars> (noting that Sony turned over “the complete server logs from the company’s *Everquest 2* MMORPG.”).

39. See Rijacki, Comment to *Sony and Our Personal Data*, STATION (Feb. 16, 2009, 7:06 AM), http://forums.station.sony.com/eq2/posts/list.m?topic_id=443700 (responding to a question about what data has been shared with, “It’s all the in-game stuff, tells, say, emotes, group chat, guild chat, channel chat, etc [sic] (covered by the EULA, btw, that they save it and can do with it what they want).”). The poster also surmised: “Looks like they’re also giving demographics on the players, I hope by character name only . . .” *Id.* See also *How Everquest II Helps Train Soldiers*, GAMEPOLITICS (Jan. 26, 2011), <http://gamepolitics.com/2011/01/26/how-everquest-ii-helps-train-soldiers> (asserting that “Sony provided researchers with anonymous player communications, game logs, and other game data.”). *But see* *SOE Contributes Gaming Data to Research Project*, EVERQUEST II, <http://www.everquest2.com/news/read/022009/2074> (last visited June 6, 2012) (emphasizing that “the server logs were scrubbed of all PII (Personally Identifiable Information) prior to being provided to the researchers, including chat log content”). These conflicting reports indicate that while the EverQuest data probably did not include chat logs, the EULA provides that it could easily have included such logs. This bears emphasis. License agreements are consistently upheld by courts short of the glaringly

information pursuant to the EULA, as a condition of user access to the virtual world community.⁴⁰ The information is gathered in compliance with commercial standards and general contract law, for traditional commercial and customer service uses.⁴¹ Secondary data sets in virtual worlds are extremely attractive to researchers because they are so large and so comprehensive. Gathering so much information in such detail is expensive and would be cost prohibitive to the researcher absent secondary research databases.⁴²

2. *Qualitative Research Methodologies*

Research can also be divided into the categories of qualitative and quantitative research. Qualitative research is founded on contextual interpretation.⁴³ Techniques for gathering qualitative data sets include interviews, nonreactive observation, collection of personal documents, and participant

obvious. *See, e.g.*, Davidson & Assocs. v. Jung, 422 F.3d 630, 639 (8th Cir. 2005) (“By signing the TOUs and EULAs, Appellants expressly relinquished their rights to reverse engineer.”); Bowers v. Baystate Techs, Inc., 320 F.3d 1317, 1325–26 (Fed. Cir. 2003) (detailing that private parties are able to contract out of exemptions afforded to them under the Copyright Act). *But see* Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 605–07 (E.D. Pa. 2007) (noting that the contract was procedurally unconscionable despite the fact that Bragg was an attorney). The concern is that what EULAs provide, their authors will take advantage of. *See Terms of Service, SECOND LIFE*, <http://secondlife.com/corporate/tos.php> (last visited June 6, 2012) [hereinafter *Second Life Terms of Service*] (“We may suspend or terminate your Account if we determine in our discretion that such action is necessary or advisable to comply with legal requirements or protect the rights or interests of Linden Lab, the Second Life community or any third party.”). Linden Lab used its privileges under a comparable section of the Terms of Use when Bragg was a user of Second Life and Linden Lab froze his account and confiscated all of his virtual assets.

40. *See* discussion *infra* Part III.B.2 (describing the influence of contract law on virtual worlds research).

41. This recording serves different commercial purposes. Chat logging assists with customer service disputes, while logging economic transactions permits the game gods to protect the money supply against virtual counterfeiter.

42. *See* Bailey, *supra* note 37, at 110 (“[A]n individual researcher is unlikely to possess the resources (even with a large grant) to collect data on 3,000 or more cases and so must often rely on secondary data . . .”). *See also* Magnus Johansson & Harko Verhagen, *And Justice for All—The 10 Commandments of Online Games, and Then Some . . .*, in PROCEEDINGS OF DIGRA NORDIC 2010 (Jan. 2010) [hereinafter *Online Commandments*], available at http://www.digra.org/dl/display_html?chid=10343.53531.pdf (detailing research on social rules of conduct in MMOGs and FPS used by clans or guilds). The researchers used online searches and did not seek consent of participants as the data could easily be gathered on already public sites.

43. *See* Bailey, *supra* note 37, at 99 (“[Q]ualitative researchers study things in their natural settings, attempting to make sense of or interpret these things in terms of the meanings people bring to them.”). *See also* Natascha Karlova, *Research Spotlight: Virtual Worlds, Avatars, and Trust*, CRITICAL GAMING PROJECT (Jan. 25, 2011), <https://depts.washington.edu/critgame/wordpress/2011/01/research-spotlight-virtual-worlds-avatars-and-trust> (detailing a research project to investigate issues of trust and credibility in Second Life, specifically on Health and Politics). The researchers created their own avatars and interacted with Second Life residents, specifically five community leaders in the Health community and five leaders in the Political community in Second Life. *Id.* The researchers conducted interviews ranging from ninety minutes to five hours, made approximately one hundred hours of observation, and spent over twelve hours shadowing selective participants. *Id.*

observation.⁴⁴ Numerous prominent researchers have used qualitative methods to study virtual worlds. Thomas Malaby, Constance Steinkuehler, Celia Pearce, Tom Boellstorff, Mia Consalvo, and Lisa Galarneau have all published groundbreaking studies incorporating qualitative methodologies.⁴⁵

The participant observer method is particularly common in virtual worlds research,⁴⁶ and so this discussion will focus on that technique. Participant observers establish a presence and reputation in-world,⁴⁷ and virtual world communities are often willing and eager to assist the researcher in exploring the world.⁴⁸ Observers may interview subjects in-world, in realspace, or both.⁴⁹ They often accompany subjects as the subjects go about their virtual lives.⁵⁰ Participant observers record their own observations, possibly in addition to those of others.⁵¹ The participant observation methodology thus relies in part on the observer finding a role within the group and the group consenting to being observed.

Qualitative research involves deep investment in community norms and the gradual development of trust between researcher and community.⁵² Just as realspace sociologists carefully establish communications and build trust with populations they desire to study, so virtual world qualitative researchers carefully

44. See CHRIS MANN & FIONA STEWART, INTERNET COMMUNICATION AND QUALITATIVE RESEARCH: A HANDBOOK FOR RESEARCHING ONLINE 74–98 (2000) (describing the various techniques in detail).

45. See TOM BOELLSTORFF, COMING OF AGE IN SECOND LIFE: AN ANTHROPOLOGIST EXPLORES THE VIRTUALLY HUMAN (2008); GAMES, LEARNING, AND SOCIETY (Constance Steinkuehler et al. eds., 2012); THOMAS M. MALABY, MAKING VIRTUAL WORLDS: LINDEN LAB AND SECOND LIFE (2006); Lisa Galarneau, *Online Games for 21st Century Skills*, in GAMES AND SIMULATIONS IN ONLINE LEARNING: RESEARCH AND DEVELOPMENT FRAMEWORKS (David Gibson et al. eds., 2007); Mia Consalvo & Nathan Dutton, *Game Analysis: Developing a Methodological Toolkit for the Qualitative Study of Games*, 6 GAME STUDS. 1 (2006).

46. See MANN & STEWART, *supra* note 44, at 88 (“Certainly data that give insight into online groups from the perspective of those involved are becoming increasingly available. At some level all researchers who comment on virtual communities of which they are part are participant observers.”).

47. See *id.* (“Participant observation is, above all, concerned with access.”); see also Karlova, *supra* note 43 (“In order to understand the perspectives of our participants, we all created avatars, modified them, explored in-world, and found a wide range of communities in which we developed relationships with other residents.”).

48. See discussion *infra* Part III.B.1.b (describing the eagerness of virtual community members to aid a researcher).

49. See MANN & STEWART, *supra* note 44, at 87–91 (describing the process of participant observation).

50. See *id.*

51. See Bailey, *supra* note 37, at 99 (listing the empirical materials used in qualitative study as “case study, personal experience, introspection, life story, interview, and observational, historical, interactional, and visual texts”).

52. See MANN & STEWART, *supra* note 44, at 90 (“[S]ome participant observers may have made limited assumptions about the character of online communities because they had never penetrated beyond the most public and easy-to-find interactive ‘rooms’ and had only interacted with other ‘newbies.’ . . . ‘[R]egulars who seek a quiet place to convene with friends build their own rooms, which allows them to control access’. [sic] It is only researchers who both ‘find’ these secret places, and who then negotiate access, who begin to grasp the boundaries of the community.”).

build trust with online groups.⁵³ For example, a “guild” is a group in a virtual world that shares common purposes, goals, and communications channels.⁵⁴ Guilds socialize, go on raids together, fight as a unit against interlopers, squabble, and often fracture, split, and grow anew.⁵⁵ Guild structure is of great interest to researchers studying group interaction online, and thus qualitative researchers often approach prominent guilds and develop relationships with the guilds and their leaders.⁵⁶ Once trust is established, researchers may follow guilds during activities and raids, or even join the guild in order to have access to guild-only chat channels. So important is community and trust that researchers will sometimes follow one community across multiple virtual environments.⁵⁷

3. *Quantitative Research Methodologies*

Quantitative methodology includes the computational analysis of large data sets.⁵⁸ In virtual worlds research, quantitative data sets can include all conduct or

53. See *id.* at 90 (quoting Paul Hodkinson, *The Goth Scene as Trans-Local Subculture* (2000) (unpublished)) (“Regardless of one’s involvement in the [community] scene off-line, acceptance in their exclusive on-line forums can take considerable time to earn. Furthermore, it requires the learning of particular sets of norms for on-line behaviour distinct from the values of the subculture as a whole.”); see also Karlova, *supra* note 43 (“Prior to the interviews, we obtained informed consent from our participants. However, we did not receive consent from them to collect and publish their images, so . . . we use[d] generic, stock avatar images . . . to maintain good relationships with them.”).

54. See *Playing Together*, WORLD WARCRAFT, <http://us.battle.net/wow/en/game/guide/playing-together> (last visited June 6, 2012) (“Parties and raids are temporary alliances, but guilds are persistent groups of characters who regularly play together and who generally prefer a similar gaming style.”). The page goes on to explain “guild chat,” “ranks,” “guild banks,” and cohesion indicators like “guild tabards.” *Id.*

55. See *id.*

56. See, e.g., Lisa Poisso, *15 Minutes of Fame: Anthropologist Digs into WoW*, WOW INSIDER (Jan 6, 2009, 5:00 PM), <http://wow.joystiq.com/tag/Alex-Golub> (describing anthropologist Alex Golub’s research on guild interactions); see also *Online Commandments*, *supra* note 42, at 2 (detailing one of the most important issues to be addressed, that of grievers, which are defined as “[b]ullies prepared to use force or other unpleasantness to get their way or be noticed.”). This study was quantitative but further highlights the importance of social rules, particularly trust, in online games ranging from World of Warcraft and Star Wars Galaxies, to Counter Strike and Call of Duty. See *id.*

57. For example, Dr. Celia Pearce studied the devotees of Uru Online, a virtual world based on the Myst series of video games. Uru was canceled, and the Uru community dispersed to several different virtual worlds. Some community members settled in Second Life; most settled in virtual world There.com. Still others attempted to resurrect the defunct Uru world as the intellectual property of the world was passed from one publisher to another in an attempt to bring the world to market successfully. Now that There.com itself has been canceled, the Uru diaspora studied by Pearce will likely continue to new virtual worlds. See Joshua A.T. Fairfield, *The End of the (Virtual) World*, 112 W. VA. L. REV. 53 (2009).

58. See Bailey, *supra* note 37, at 109 (“Many extant quantitative techniques (particularly inductive statistics) can only be used on data collected with a rigorous and sufficiently large probability sample, generally a random sample of some sort.”). For an exciting and new approach to analysis of large data sets, see Brent Harrison & David L. Roberts, *Using Sequential Observations to Model and Predict Player Behavior*, PROCEEDINGS OF THE 2011 FOUNDATIONS OF DIGITAL GAMES CONFERENCE 91 (2011), <http://www.csc.ncsu.edu/faculty/robertsd/papers/achievements-fdg-10.pdf> (detailing the benefits of a data-driven approach to player modeling over the more traditional

communication in a virtual world.⁵⁹ Although quantitative research in virtual worlds has been less prevalent than qualitative research, prominent and important studies using both primary and secondary quantitative data sets have now been published.

Quantitative research in virtual worlds was pioneered and most successfully popularized by the father of virtual worlds academic research, Ted Castronova, an economist who first established the value of in-world trade within the virtual world EverQuest.⁶⁰ Leading primary quantitative researchers include Nic Ducheneaut, Nick Yee, Bob Moore, and Eric Nickell, who have variously collaborated on a series of papers published under the aegis of the PlayOn project conducted at the Palo Alto Research Center (PARC).⁶¹ The PlayOn project combined online surveys, information collected by Facebook applications, and in-world data gathering to enable quantitative analysis on issues ranging from space design and social skills acquisition to guild formation and group conduct.⁶²

Secondary quantitative research has also risen in prominence, largely due to the work of Professor Dmitri Williams of the University of Southern California Annenberg School for Communication and Journalism.⁶³ Williams negotiated with Sony Online Entertainment, creator of the virtual world EverQuest II, to receive large amounts of data collected via the game servers.⁶⁴ Williams then combined the secondary data with primary survey data (for which traditional research consent was obtained), and has collaborated with numerous coauthors to study a wide range of virtual world phenomena based on the combined data sets.⁶⁵

approaches of user surveys, small-scale modeling, and small-scale observation). The study used sequential observations to predict a user's behavior based on an analysis of prior users in similar situations. The study focused on the World of Warcraft, specifically the Armory (a public online database of all avatars and their activities). This method of data-driven research provided the researchers a preferable method of data gathering and analysis because the research covered more player behavior, could be updated faster, and was more adaptable, particularly with the constant expansion of virtual worlds. *Id.* at 6. The research also included more users than traditional methods. *Id.* at 1. Sequential observations prevented biases in traditional research, such as "social desirability bias" as well as eliminating knowledge engineering. *Id.* The study did not obtain informed consent because the information gathered was public and harvested from an online database.

59. See Timmer, *supra* note 38 (describing the content of one quantitative game data set).

60. See Castronova, *supra* note 4.

61. See *Publications*, PARC, <http://www.parc.com/publications> (last visited June 6, 2012) (listing all PARC-associated papers).

62. See *PlayOn Authors Archive*, PARC, <http://blogs.parc.com/blog/author/playon> (last visited June 6, 2012) (listing all PlayOn papers).

63. See Dmitri Williams, *Research*, DMITRI WILLIAMS, <http://dmitriwilliams.com/research.html> (last visited June 6, 2012) (describing Dr. Williams' research).

64. See Timmer, *supra* note 38 (describing Dr. Williams' receipt of SOE's data).

65. For a list of over forty publications, reviews, presentations, and essays, see Williams, *supra* note 63.

B. Law

The law governing human subjects research in virtual worlds is wide-ranging and complex. All human subjects research funded or supported by the U.S. federal government must comply with regulatory standards regarding informed consent and minimization of harm.⁶⁶ Researchers also face the challenge of conducting research within a virtual space almost entirely governed by copyright and the contracts that govern copyright, termed End User License Agreements (EULAs) or Terms of Service (TOS).⁶⁷ When researchers record their subjects, they must take care not to run afoul of ubiquitous copyrights that inhere in the environment and the avatars that populate such spaces.⁶⁸ In addition, certain research methodologies may implicate privacy law more broadly, including privacy torts and privacy statutory regimes. This Subpart will examine each of these areas of law in turn.⁶⁹

1. The Belmont Report and Federal Common Rule

Modern law governing human subjects research grew out of public moral outrage concerning human rights abuses during World War II.⁷⁰ The Nuremberg Trials exposed these abuses and resulted in the influential Nuremberg Code.⁷¹ The Code's primary mandate to researchers is that "[t]he voluntary consent of the human subject is absolutely essential" and that subjects should be protected from harm.⁷² In 1964 the World Medical Association passed the *Declaration of Helsinki*,⁷³ setting out ethical principles for the medical community regarding research involving human subjects. It charges researchers with the responsibility to

66. 45 C.F.R. § 46.103 (2011).

67. See Joshua A.T. Fairfield, *Anti-Social Contracts: The Contractual Governance of Virtual Worlds*, 53 MCGILL L.J. 427 (2008) (arguing that consumer contracts cannot constitute the entire social contract of a virtual world); Erez Reuveni, *On Virtual Worlds: Copyright and Contract Law at the Dawn of the Virtual Age*, 82 IND. L.J. 261, 287 (2007) (arguing that company-drafted consumer contracts do constitute the new social contract of online worlds).

68. See discussion *infra* Part III.B.2 (explaining the limited effectiveness of the Fair Use defense to research copyright infringement as well as other consequences of copyright infringement during virtual worlds research).

69. See discussion *infra* Part III.B.3 (describing the privacy implications of virtual worlds research).

70. See Robin Fretwell Wilson, *Estate of Gelsinger v. Trustees of University of Pennsylvania: Money, Prestige, and Conflicts of Interest in Human Subjects Research*, in HEALTH L. & BIOETHICS 229, 235 (Sandra H. Johnson et al. eds., 2009) (describing the callous research rationale that "people in the [Nazi] camps were going to die anyway, so let's experiment on them").

71. See *Regulations and Ethical Guidelines: The Nuremberg Code*, OFF. HUM. SUBJECTS RES., <http://ohsr.od.nih.gov/guidelines/nuremberg.html> (last visited June 6, 2012) [hereinafter *The Nuremberg Code*] (addressing the necessity of requiring the voluntary consent of human subject participants and the personal responsibility of the investigator for the quality of the consent).

72. MCKEE & PORTER, *supra* note 33, at 33 (quoting the Nuremberg Code).

73. See *Regulations and Ethical Guidelines: The Declaration of Helsinki*, OFF. HUM. SUBJECTS RES., <http://ohsr.od.nih.gov/guidelines/helsinki.html> (last visited June 6, 2012).

“protect the well-being, privacy, and confidentiality of subjects, to obtain voluntary informed consent, and to assess the risks and benefits of research with the subjects’ well-being in mind.”⁷⁴ The most recent version “calls for prior approval and ongoing monitoring of research by independent ethical review committees.”⁷⁵ Still more recently, the infamous Tuskegee Study⁷⁶ prompted 1974 legislation creating the national Commission for the Protection of Human Subjects of Biomedical and Behavioral Research.⁷⁷ The Commission crafted *The Belmont Report*, the seminal treatise on ethical principles and guidelines for the protection of human subjects.⁷⁸

The Belmont Report remains an influential document because it “is a statement of basic ethical principles and guidelines that should assist in resolving the ethical problems that surround the conduct of research with human subjects.”⁷⁹ The report is not a regulatory statute and therefore does not have legal force in its own right. The report was not meant to be a legally enforceable document. Its purpose and effect is to function as a guideline for conducting research on human subjects. It forms the basis for the statutory regimes that are described below.⁸⁰ The authors of the report explained its significance:

[Specific regulatory codes] consist of rules, some general, others specific, that guide the investigators or the reviewers of research in their work. Such rules often are inadequate to cover complex situations; at times they come into conflict, and they are frequently difficult to interpret or apply. Broader ethical principles will provide a basis on which specific rules may be formulated, criticized and interpreted.⁸¹

As such, *The Belmont Report* is highly significant when analyzing the law governing human subjects research. Without examining the report, it is not possible to

74. See MCKEE & PORTER, *supra* note 33, at 33.

75. OFFICE OF REGULATORY AFFAIRS, INSTITUTIONAL REVIEW BOARD OF GEORGETOWN UNIVERSITY POLICIES AND PROCEDURES MANUAL 1 (2008), available at <http://ora.georgetown.edu/irb/Policies/Chapters.pdf>.

76. The Tuskegee Study researched the effects of untreated syphilis in a group of African American men beginning in the 1950s and continuing into the early 1970s. See Robin Fretwell Wilson, *supra* note 3. The researchers purported to treat the men, but never disclosed to them that they continued to suffer from syphilis, which penicillin could treat. *Id.*

77. See *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects Research*, OFF. HUM. SUBJECTS RES., <http://ohsr.od.nih.gov/guidelines/belmont.html> (last visited June 6, 2012).

78. *Id.*

79. *Id.*

80. See, e.g., 32 C.F.R. § 219.101 (2012) (implementing the guidelines of *The Belmont Report* for research on human subjects for the Department of Defense); see also 21 C.F.R. § 50.20 (2012) (outlining the requirements of consent for human subjects research by the FDA); DEPARTMENT OF DEFENSE INSTRUCTION 3216.02, PROTECTION OF HUMAN SUBJECTS AND ADHERENCE TO ETHICAL STANDARDS IN DOD SUPPORTED RESEARCH (2011), available at <http://www.dtic.mil/whs/directives/corres/pdf/321602p.pdf>.

81. See *The Belmont Report*, *supra* note 77.

provide a holistic view of the various statutory guidelines that hold legal sway over research decisions.

The Belmont Report focuses on the respect for persons principle (often termed autonomy for brevity), the beneficence principle, and the justice principle.⁸² The autonomy principle promotes respect for persons by requiring that potential research subjects give fully informed consent.⁸³ The beneficence principle requires researchers to minimize potential harm and to balance unavoidable risk of harm with potential benefit.⁸⁴ The justice principle requires that the benefits of research be equitably distributed.⁸⁵

The Belmont Report in turn lays the ethical groundwork for the Common Rule, which is implemented in federal regulations. Today, many federal agencies have adopted the Common Rule or some slight modification of it.⁸⁶ Some agencies adopt all parts of the rule; others adopt some subset of the rule's components.⁸⁷ Agencies that adopt only part of the Common Rule as a regulation may nevertheless require compliance with all subparts of the rule as part of implementing instructions.⁸⁸ Still other agencies are bound by presidential order. For example, in 1994 President Clinton required all agencies to "review present practices to assure compliance [with the Common Rule] and to cease immediately sponsoring or conducting any experiments involving humans that do not fully comply with the Federal Policy."⁸⁹

The Common Rule has four components.⁹⁰ Subpart A sets forth the basic rules and definitions governing human subjects research.⁹¹ Subparts B through D provide additional protections for vulnerable research populations: pregnant women, in vitro fertilization, fetuses, prisoners, and children.⁹²

82. See MCKEE & PORTER, *supra* note 33, at 33 (listing the three foci of *The Belmont Report*).

83. See *id.* ("[I]ndividuals should be treated as autonomous agents.")

84. See *id.* (listing "do not harm" and "maximize possible benefits and minimize possible harms" as "complementary expressions of beneficent actions").

85. See *id.* (noting that the "question of justice" is about "fairness in distribution").

86. See Henry T. Greely, *Neuroscience and Criminal Justice: Not Responsibility but Treatment*, 56 U. KAN. L. REV. 1103, 1126 n.82 (2008) ("The Common Rule is so called because it was adopted in common by over sixteen federal agencies, almost all of the agencies that perform or fund human subjects research. Each agency is bound by its own version of the Common Rule, but most of them parallel closely the HHS rule, codified at 45 C.F.R. § 46 . . .").

87. *Id.* at 1126.

88. See Jennifer J. Kulynych, *The Regulation of MR Neuroimaging Research: Disentangling the Gordian Knot*, 33 AM. J.L. & MED. 295, 303 n.45 (2007) (citing 45 C.F.R. § 46.103(b)(1) (2006)) ("Any institution that does not elect to apply the Common Rule to otherwise unregulated research must nonetheless specify in its assurance the principles that it will follow in the oversight of such research.")

89. See Memorandum on Research Involving Human Subjects, 1 PUB. PAPERS 281 (Feb. 17, 1994).

90. Greely, *supra* note 86, at 1126.

91. *Id.*

92. *Id.*

The Common Rule regulates research that both involves human subjects and is federally funded or supported.⁹³ Research means “a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.”⁹⁴ The types of data subject to Common Rule regulation are found in the rule’s definition of human subjects.⁹⁵ Human subjects are living individuals from whom a researcher “obtains [certain types of d]ata.”⁹⁶ Thus, the rule clearly governs primary research data: information that a researcher obtains directly from the research subject or by interacting with the research subject.

The regulations do exempt some activities from regulation.⁹⁷ Important exemptions include education activities,⁹⁸ educational tests,⁹⁹ educational tests on public officials,¹⁰⁰ publicly accessible existing data sources,¹⁰¹ existing data sources not publicly accessible *if* recorded by the investigator and scrubbed of Personally Identifiable Information (PII),¹⁰² evaluation of public benefit programs,¹⁰³ and food safety evaluation.¹⁰⁴ Only two of these exemptions are relevant to this Article: publicly accessible existing data sources and existing data sources not publicly accessible *if* recorded by the investigator and scrubbed of PII.

One important question is whether secondary research data gathered by a third party and then licensed to the researcher is likewise covered by the Common Rule. These sets would only fall within the meaning of the publicly available exemption if the process of licensing the data renders it public. Otherwise, commercial data sets will fall under the regulations if “obtains” refers to either direct or secondary collection of data. Neither the phrase “publicly available” nor the word “obtains” is defined in the regulations,¹⁰⁵ although some guidance on biological specimen collection has defined “obtaining.”¹⁰⁶ Researchers who receive

93. See 45 C.F.R. § 46.103(b) (2011) (requiring that departments or agencies only conduct or support research at an institution that is reviewed and approved by the IRB provided for in the Federalwide Assurance (FWA), a document each research institution files with the Office for Human Research Protections in order to maintain its status as a valid recipient of federal research funds).

94. *Id.* § 46.102(d).

95. See *id.* § 46.102(f).

96. *Id.* The types of data referred to here are explained below. See *supra* notes 33–39 and accompanying discussion.

97. See 45 C.F.R. § 46.101(b).

98. *Id.* § 46.101(b)(1).

99. *Id.* § 46.101(b)(2).

100. *Id.* § 46.101(b)(3).

101. *Id.* § 46.101(b)(4).

102. *Id.* § 46.101(b)(4).

103. *Id.* § 46.101(b)(5).

104. *Id.* § 46.101(b)(6).

105. See *id.* § 46.102 (omitting “publicly available” and “obtains” from the definitions section of the regulation). However, “private information” is defined in the regulations. See *infra* note 131–33 and accompanying text (explaining the definition of “private information” and its applicability to this Article).

106. See Office for Human Research Prots., *Guidance on Research Involving Coded Private*

secondary data from a third party acquire and possess the information just as readily as primary researchers do.¹⁰⁷ Therefore, the regulations should apply to secondary analysis as well as primary data collection. Guidance from the Office for Human Research Protections (OHRP) regarding analogous coded private information,¹⁰⁸ biological specimens,¹⁰⁹ and tissue repositories¹¹⁰ agrees.

The OHRP excludes the use of some coded private information or biological specimens from the definition of human subjects research.¹¹¹ The exclusion operates when coded private information is unidentifiable, either because the investigator lacks the key to decode the information and reveal the subjects' identities, or because the investigator has entered into an agreement prohibiting the investigator from making the key public until the subjects are deceased.¹¹² The exclusion applies only to coded private information and biological specimens that have been collected for purposes *other than research*. Because of this, the analogy to secondary data sets is clear. If researchers use data collected for commercial purposes, they must be sure that the information is coded and that they either cannot decode it or agree not to decode it while subjects are still alive.

OHRP guidance on tissue repositories, a different but analogous type of secondary research data set, suggests the same answer.¹¹³ OHRP says that tissue repositories consist of three components: the collector, the repository facility, and the recipient investigators.¹¹⁴ In the secondary data analysis of virtual worlds, the

Information or Biological Specimens, HHS.GOV (Oct. 16, 2008), <http://www.hhs.gov/ohrp/policy/cdebiol.html> [hereinafter *Guidance*] (describing the term). Specifically, the guidance document explains:

Obtaining identifiable private information or identifiable specimens includes, but is not limited to:

1. using, studying, or analyzing for research purposes identifiable private information or identifiable specimens that have been provided from any source; and
2. using, studying, or analyzing for research purposes identifiable private information or identifiable specimens that were already in the possession of the investigator.

Id.

107. *Id.* See *supra* notes 39–40 and accompanying text.

108. Coded private information is PII that has been coded such that an investigator could not identify the individuals included in the data without a special key. See *Guidance, supra* note 106 (defining coded private information). Coded private information is considered PII because an investigator could readily, albeit indirectly, identify the subject by using the key. *Id.*; see also 45 C.F.R. § 46.102(f).

109. Biological specimens are specimens that, although potentially originating with a human being, cannot be linked back to that living individual. In the context of the OHRP memorandum cited here, “biological specimens” refers to specimens taken for some purpose other than research. *Guidance, supra* note 106.

110. Tissue repositories are facilities that “collect, store, and distribute tissue materials for research purposes.” Office for the Prot. from Research Risks, *Issues to Consider in the Research Use of Stored Data or Tissues*, HHS.GOV (Nov. 7, 1997), <http://www.hhs.gov/ohrp/policy/reposit.html> [hereinafter *Issues to Consider*].

111. See *Guidance, supra* note 106 (explaining the exclusion, and differentiating the exclusion from the exemptions in 101(b)).

112. *Id.*

113. See *Issues to Consider, supra* note 110 (providing a chart showing where in the secondary research process IRB review, informed consents, and local agreements apply).

114. *Id.*

game gods are the collectors. By analogy to the tissue repository rules, the repository facility would be the game gods' storage servers. The recipient investigators, under this analogy, would be the researchers analyzing the data. This Article does not argue that game god data is governed by the rules governing tissue repository rules, but rather that the tissue repository rules provide a useful analogy for analyzing game god collection of data for use by researchers. OHRP mandates review by institutional review boards (IRBs), informed consent, submittal agreement,¹¹⁵ and assurance compliance at the collection stage.¹¹⁶ All of these compliance procedures rest on the game gods in secondary virtual world analysis. Indeed, OHRP suggests that another IRB review, sample informed consent, a certificate of confidentiality, and another assurance of compliance would be required in the game gods' storage and management capacity.¹¹⁷ Recipient agreement¹¹⁸ and local policies would fall to the recipient investigators.¹¹⁹

Social science researchers and human subjects protection experts have endlessly debated whether social science research should fall within human subjects research regulations.¹²⁰ OHRP guidance on oral histories, which has been revised multiple times,¹²¹ is instructive. Over three years of discussion on the applicability of human subjects research rules to oral history interviews, an OHRP

115. A submittal agreement "should require written informed consent of the donor-subjects utilizing an informed consent document approved by the local IRB." *Id.* Additionally, it should "contain an acknowledgment that collectors are prohibited from providing recipient-investigators with access to donor-subjects or to information through which the identities of donor subjects may readily be ascertained." *Id.*

116. *Id.*

117. *Id.*

118. In the cell repository context, the recipient agreement requires language specifically designated by OHRP. *Id.* This language includes an acknowledgement "that the conditions for use of this research material are governed by the cell repository Institutional Review Board (IRB) in accordance with Department of Health and Human Services regulations . . ." *Id.* The recipient must also agree "to comply fully with all such conditions and to report promptly . . . any proposed changes in the research project and any unanticipated problems involving risks to subjects or others." *Id.* The recipient also agrees to "remain[] subject to applicable State or local laws or regulations and institutional policies" as well as to obtain a completely new IRB approval for any additional, non-agreed-to research purpose. *Id.*

119. *Id.*

120. See, e.g., Jeffrey Cohen, *OHRP and Oral History*, HRPP BLOG (Nov. 28, 2006), <http://hrpp.blogspot.com/2006/11/ohrp-and-oral-history.html> (discussing the ongoing discussion and clarification of whether any or all oral history investigations constitute human subjects research); *Updated UT Policies & Position Papers*, U. TEX., http://www.utexas.edu/research/rsc/humansubjects/special_topics/policy_updates.html (last visited June 6, 2012) (listing marketing, public data sets, journalism, social security numbers, and oral history among topics that have required continued discussion and policy revision).

121. See Cohen, *supra* note 120 ("[At a research conference], Dr. Carome finally clarified OHRP's position on oral history. As many of you know, in 2003 Dr. Carome wrote a letter stating that OHRP concurred with the position that oral history activities in general do not involve research as defined by the HHS regulations.").

official clarified the inclusion of oral history activities in human subjects research.¹²² In 2006 that official clarified that the regulatory definition of human subjects research is the paramount consideration.¹²³ Despite the general classification of oral history as exempt from human subjects research regulation,¹²⁴ oral history activities conducted within the context of the regulatory definition are nonetheless subject to those regulations.¹²⁵

This reading is supported by the inclusion of category (5) in the categories of research eligible for expedited review by the Department of Health and Human Services (DHHS).¹²⁶ Category (5) includes “[r]esearch involving materials (data, documents, records, or specimens) that have been collected or will be collected solely for nonresearch purposes (such as medical treatment or diagnosis).”¹²⁷ This is exactly the definition of secondary research gathered by game gods and analyzed by researchers after the fact.¹²⁸ And the advanced notice of proposed rule making (ANPRM) expressly considers secondary research to potentially fall under human subjects constraints.¹²⁹

122. See *Clarification of OHRP’s Position on Oral History Information*, ORAL HIST. ASS’N (Nov. 22, 2005), http://www.utexas.edu/research/rsc/humansubjects/forms/michael_carome_updated.pdf; Linda Shopes, *Human Subjects and IRB Review*, U. TEX., <http://www.oralhistory.org/do-oral-history/oral-history-and-irb-review> (last visited June 6, 2012); *Outline of October 30, 2003 Discussion with Dr. Michael Carome, Associate Director, HHS-OHRP, Regarding Oral History, Qualitative Interviews, and Human Subjects Research*, U. TEX., http://www.utexas.edu/research/rsc/humansubjects/forms/michael_carome.pdf (describing the various viewpoints on the inclusion of oral history techniques in human subjects research).

123. See Cohen, *supra* note 120 (citing Dr. Michael Carome, OHRP, Panel Remarks at PRIM&R HRPP 2006: When Is It Human Subjects Research? (Nov. 17, 2006)) (“It is not the methodology that determines whether an activity is human subjects research, but whether it meets the regulatory definition of research—a systematic investigation designed to develop or contribute to generalizable knowledge.”). Cohen goes on to explain, “the determination as to whether an oral history activity is human subjects research is based on how it is conducted and the purpose for which the activity was conducted.” *Id.*

124. See *Clarification of OHRP’s Position on Oral History Information*, *supra* note 122 (“OHRP has taken the position that the activity of performing an oral history in and of itself does not make the activity research as defined by 45 C.F.R. § 46.102(d).”).

125. See *id.* (“For example, OHRP could have stated that activities that involve taking a medical history, a blood draw for serum chemistries, a chest x-ray, or a CT scan of the head *in general* do not involve human subjects research; however, when investigators conducting non-exempt human subjects research use such procedures, the research must be reviewed by an IRB if the research is conducted or supported by HHS or conducted under an applicable OHRP-approved assurance.”) (emphasis added).

126. See Protection of Human Subjects: Categories of Research That May Be Reviewed by the Institutional Review Board (IRB) Through an Expedited Review Procedure, 63 Fed. Reg. 60364 (Nov. 9, 1998) [hereinafter Protection of Human Subjects] (listing nine specific categories of research eligible for expedited review).

127. *Id.* at 60366.

128. It is important to note that the parenthetical referring to clinical settings represents an indication of extremely common secondary research settings, not an exclusive description of what types of nonresearch settings qualify for the category.

129. See discussion *infra* Part III.B.1.e.

It is important not to misunderstand this point. Not all activities listed as qualifying for expedited review constitute human subjects research. If activities included under the possible expedited review process do not meet the regulatory definition, they will not be considered human subjects research. But it is equally clear from the text that analysis of secondary data sets was contemplated in the regulation as one possible type of human subjects research—that is, that analysis of secondary data sets is not per se excluded.

The inclusion of category (5), describing just the sort of secondary analysis at issue in virtual worlds secondary research, shows that the Common Rule is equally applicable to primary and secondary researchers. Reinforcing this reading is the regulation's definition of research to include "[a]ctivities which meet this definition . . . whether or not they are conducted or supported under a program which is considered research for other purposes."¹³⁰

The researcher must also obtain "[d]ata through intervention or interaction with the individual" or "[i]dentifiable private information" in order for the Common Rule to apply.¹³¹ Private information is either "information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place" or "information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public."¹³² Private information must be individually identifiable—that is, the "identity of the subject is or may readily be ascertained by the investigator or associated with the information . . . in order for obtaining the information to constitute research involving human subjects."¹³³

The federal government has created a delegated authority process by which research proposals are approved and continuously reviewed for compliance with federal research regulations.¹³⁴ Approval of human subjects research rests primarily with IRBs, which are made up of at least five members,¹³⁵ including at least one person whose primary concerns are scientific and one whose primary concerns are nonscientific.¹³⁶ Research institutions usually maintain their own

130. 45 C.F.R. § 46.102(d) (2011).

131. *Id.* § 46.102(f)(2).

132. *Id.*

133. *Id.*

134. If an institution conducted research without any use of federal grants or support, it might escape IRB review for that research. However, most universities require all research to go through the IRB approval process described below, whether federally funded or not. *See, e.g., Statement of Policies and Procedures Governing the Use of Human Subjects in Research at Harvard University*, HARVARD U. (Sept. 22, 2003), <http://www.fas.harvard.edu/~research/greybook/humsubs.html> (requiring conformance with the Common Rule regardless of the funding source). Researchers are thus prudent to comply with all federal regulations to ensure that their research will be approved by their institutional IRB.

135. 45 C.F.R. § 46.107(a) (2011).

136. *See id.* § 46.107(c); *id.* § 46.107(d) (requiring diverse viewpoints). In addition, all members should have the competence necessary to review the proposed research. *See id.* § 46.107(a) ("The IRB shall be sufficiently qualified through the experience and expertise and qualifications of its

affiliated IRBs.¹³⁷ Some public institutions and many private companies also take advantage of private IRBs.¹³⁸ Private IRBs are for-profit organizations that offer researchers quicker turnaround time and expertise in specific research areas.¹³⁹

An IRB is responsible for the approval and ongoing supervision of human subjects research conducted by the institution or its agents.¹⁴⁰ The IRB may do this through a regular review procedure that requires a majority of a quorum of the IRB,¹⁴¹ or through expedited review that requires only one member of the IRB to approve the proposal.¹⁴² If a research proposal is disapproved, the researcher may make modifications and resubmit the proposal.¹⁴³ There is no limit on the number of times the researcher may resubmit, though time and cost may impose practical limits.¹⁴⁴ The IRB may take advantage of regulations allowing IRBs to

members . . . to promote respect for its advice and counsel.”).

137. See, e.g., *Human Research Protection Program*, YALE U., <http://www.yale.edu/hrpp> (last visited June 6, 2012); *Approval of Research with Human Subjects*, WASH. & LEE U., <http://www.wlu.edu/x33135.xml> (last visited June 6, 2012); *Human Subjects Research and IRB*, U. ARIZ., <http://ocr.vpr.arizona.edu/irb> (last visited June 6, 2012).

138. See, e.g., *Institutional Review Board*, JOHNS HOPKINS SCH. PUB. HEALTH, <http://www.jhsph.edu/irb> (last visited June 6, 2012) (noting that Johns Hopkins utilizes both its own IRB and the private Western IRB).

139. See *Why Choose IRB Services?*, INST. REV. BD. SRVS., http://www.irbservices.com/irbservices/Why_IRBS.html (last visited June 6, 2012) (promising “reasonable pricing of services” and “simplified applications”).

140. See 45 C.F.R. § 46.109(a) (“An IRB shall review and have authority to approve, require modifications in (to secure approval), or disapprove all research activities covered by this policy.”).

141. See *id.* § 46.108(b) (requiring “a majority of the members” for a quorum meeting and “approval of a majority of those members present” for research to go forward).

142. See *id.* § 46.110 (outlining what categories are eligible for expedited review). Only a few specific categories of research are eligible for expedited review. See Protection of Human Subjects, *supra* note 126. Virtual worlds research may fit into the expedited review category dealing with “[r]esearch involving materials (data, documents, records, or specimens) that have been collected, or will be collected solely for nonresearch purposes.” *Id.* However, the research also probably falls into the ineligible class “where identification of the subjects and/or their responses would reasonably place them at risk of criminal or civil liability or be damaging to the subject[] financial standing, employability, insurability, reputation, or be stigmatizing . . .” *Id.* Importantly, this class is only ineligible for expedited review “unless reasonable and appropriate protections will be implemented so that risks related to invasion of privacy and breach of confidentiality are no greater than minimal.” *Id.* So, virtual worlds researchers may be eligible for expedited review if they can implement “reasonable and appropriate protections.” The expedited review guidelines specifically note that “IRBs are reminded that the standard requirements for informed consent (or its waiver, alteration, or exception) apply regardless of the type of review . . .” *Id.* This statement is interesting because it appears to mean that even the “minimal risk” research proposals are held to the same high standard of informed consent as more risky procedures ineligible for expedited review. *Id.*

143. See 45 C.F.R. § 46.109(d) (“If the IRB decides to disapprove a research activity it shall include in its written notification a statement of the reasons for its decision and give the investigator an opportunity to respond . . .”).

144. This is particularly true because some IRBs, especially private IRBs, require reimbursement for the costs of the review. See W. INST. REVIEW BD., A GUIDE FOR RESEARCHERS 66 (3d ed. 2009), available at <http://www.wirb.com/Documents/Guide%20for%20Researchers%20090605.doc> (“WIRB charges fees to cover the costs associated with the Board’s review and the related administrative responsibilities.”).

invite individuals with competence in special areas—like virtual worlds—to participate in the IRB review.¹⁴⁵ These outside experts cannot vote, but they can still provide valuable input to the IRB during decision making.¹⁴⁶

The Department of Health and Human Services (DHHS), along with its subdepartment, the Office of Human Research Protections (OHRP), requires an agreement with each institution that conducts human subjects research.¹⁴⁷ This document assures compliance with the applicable federal regulations.¹⁴⁸ To reduce duplicative applications, an institution may rely on an existing assurance agreement with DHHS, OHRP, or any successor agency.¹⁴⁹ This interdepartmental cooperation leads to the agreement's name: Federalwide Assurance (FWA).¹⁵⁰ Each institution needs only one FWA, applicable to any affiliated IRBs.¹⁵¹ While the FWA commits the institution to use registered IRBs, each IRB must itself go through a separate registration process.¹⁵²

The specific procedures and criteria for evaluating a research proposal can vary from IRB to IRB, so long as they include the main criteria listed in the Common Rule.¹⁵³ These include minimizing risk of harm to the subjects, balancing risks and benefits, equitably selecting subjects, acquiring appropriate informed consent, and providing additional safeguards for vulnerable subjects.¹⁵⁴

145. See 45 C.F.R. § 46.107(f) (“An IRB may, in its discretion, invite individuals with competence in special areas to assist in the review of issues which require expertise beyond or in addition to that available on the IRB. These individuals may not vote with the IRB.”).

146. See *id.*

147. See *id.* § 46.103(a) (“Each institution engaged in research . . . shall provide written assurance satisfactory to the department or agency head that it will comply with the requirements set forth in this policy.”).

148. These applicable regulations can include the Common Rule or other agency-specific requirements. See generally *id.* § 46 (implementing the Common Rule and principles of *The Belmont Report*). Each agency has a specific section of the Code of Federal Regulations adopting the Common Rule. See, e.g., 7 C.F.R. § 1c (2012) (Department of Agriculture); 32 C.F.R. § 219 (2012) (Department of Defense); 45 C.F.R. § 690 (2011) (National Science Foundation).

149. See 45 C.F.R. § 46.103(a) (“In lieu of requiring submission of an assurance, individual department or agency heads shall accept the existence of a current assurance, appropriate for the research in question, on file with the Office for Human Research Protections, HHS, or any successor office, and approved for federalwide use by that office.”).

150. See *id.* (approving OHRP-held FWAs for “federalwide use”).

151. See *id.* § 46.103(b) (requiring assurances include a “[d]esignation of one or more IRBs established in accordance with the requirements of this policy”).

152. See Office for Human Research Prot., *IRBs and Assurances*, HHS.GOV, <http://www.dhhs.gov/ohrp/assurances/#registernew> (last visited June 6, 2012) (setting out the steps in the registration process).

153. See, e.g., *id.* § 46.111 (listing the main criteria for approval).

154. See *id.* (same). Additional criteria may be added, or greater specificity required, depending upon the needs of the institution in question. See, e.g., Office of Regulatory Affairs, *Institutional Review Board (IRB) Policies and Procedures Manual*, GEO. U., <http://ora.georgetown.edu/irb/irbPolicies.htm> (last update June 2009); *Review Process*, IND. U. PA., <http://www.iup.edu/page.aspx?id=6663> (last visited June 6, 2012); *IRB Review Process*, U. UTAH, http://www.research.utah.edu/irb/submissions/review_process.html (last visited June 6, 2012); *WIRB Investigator Handbook*, W. INST. REV. BD., <http://www.wirb.com/Documents/Guide%20for%20Researchers.doc> (last visited June 6, 2012).

The consequences of failure to comply with federal regulations can be dire for an institution. Although IRBs approve and supervise research, the OHRP follows up to ensure that federal regulations are followed.¹⁵⁵ The OHRP can shut down entire research institutions due to an IRB's failure to provide adequate initial or continuing review.¹⁵⁶ In 1999 all human experimentation at Duke Medical Center was halted due to inadequate continuing supervision of IRB-approved human subjects research.¹⁵⁷ The main campus of Duke University, though separate from the Medical Center and subject to different IRB approval, was put on experimental probation.¹⁵⁸ This probation put a strain on social science research despite the fact that the violations were found in biomedical research projects.¹⁵⁹

The Duke shutdown appears to have been the first in a period of increased regulatory enforcement that continues today. While Duke was only the fourth institutional shutdown in ten years,¹⁶⁰ regulators shut down twenty research institutions in the following six years.¹⁶¹ Among the other institutions shut down were Johns Hopkins University,¹⁶² the University of Illinois at Chicago, the Virginia Commonwealth University, the University of Oklahoma Medical Center,¹⁶³ the University of Pennsylvania, and Georgetown University.¹⁶⁴ IRBs

155. See Office for Human Research Prot., *Compliance Oversight*, HHS.GOV, <http://www.hhs.gov/ohrp/compliance> (last visited June 6, 2012) (“OHRP’s Division of Compliance Oversight (DCO) reviews institutional compliance with the federal regulations governing the protection of human subjects in HHS-sponsored research.”).

156. See *id.* (“OHRP asks the institution involved to investigate the allegations and to provide OHRP with a written report of its investigation. The Office then determines what, if any, regulatory action needs to be taken to protect human research subjects.”).

157. See Rick Weiss, *U.S. Halts Human Research at Duke*, WASH. POST, May 12, 1999, at A1, available at <http://www.washingtonpost.com/wp-srv/national/daily/may99/duke12.htm> (“The suspension of Duke’s federal license to conduct human research is only the fourth such move by the government in nearly a decade . . .”).

158. See Christopher Shea, *Don’t Talk to the Humans: The Crackdown on Social Science Research*, LINGUA FRANCA, Sept. 2000, at 27, available at <http://linguafranca.mirror.theinfo.org/print/0009/humans.html> (“Like many places, Duke has separate IRBs for the medical school and the main campus When Duke’s medical research programs were shut down, its main campus was put on probation.”).

159. See *id.*

160. See Weiss, *supra* note 157 (“The suspension of Duke’s federal license to conduct human research is only the fourth such move by the government in nearly a decade . . .”).

161. See *Research at Canisius*, CANISIUS C., <http://www.canisius.edu/irb> (last visited June 6, 2012) (“Over the past six years, federal regulators have restricted or shut down research at more than 20 institutions for violations.”).

162. See *New IRB Tackles Re-Reviews*, JOHNS HOPKINS SCH. PUB. HEALTH, <http://www.jhsph.edu/magazineFall01/Welch.htm> (last visited June 6, 2012) (“The July 19 announcement by the OHRP shut down virtually all human subject research across the University—about 2,400 studies.”). Johns Hopkins had a single study shut down again in 2007. See Atul Gawande, Op-Ed., *A Lifesaving Checklist*, N.Y. TIMES, Dec. 30, 2007, § 4, at 8, available at <http://www.nytimes.com/2007/12/30/opinion/30gawande.html>.

163. See Donna Foote & Sharon Belgey, *Trials—and Errors*, NEWSWEEK, Aug. 5, 2001, at 38, available at <http://www.newsweek.com/2001/08/05/trials-and-errors.html> (“Last year OHRP shut

have responded to this increased OHRP enforcement by adopting more stringent standards for approval of research, particularly for social science research. Greg Koski, former director of OHRP, called this phenomenon “reactive hyper-protectionism.”¹⁶⁵ Social science experiments that traditionally flew under the IRB radar are now required by their IRBs to conform to the same approval criteria used for biomedical experimentation.¹⁶⁶

a. Autonomy

The Common Rule requires full and documented informed consent to all human subjects research.¹⁶⁷ Researchers cannot take advantage of federal support absent this consent.¹⁶⁸ Informed consent is not an intuitive term; it is a legal construction with specific requirements and regulatory consequences.¹⁶⁹ In particular, informed consent must be distinguished from contractual consent.¹⁷⁰ The informed consent standard for researchers is closer to informed consent for medical care than it is to the level of consent necessary to support a consumer contract.¹⁷¹ While informed consent to medical care and informed consent to

down all federally funded research at the campus.”).

164. See Ray Suarez, *Research Halt*, PBS (July 20, 2001), http://www.pbs.org/newshour/bb/health/july-dec01/hopkins_7-20.html (“In recent years, several other universities, including the University of Pennsylvania and Georgetown University, have been sanctioned by the government . . .”).

165. Nora Lockwood Tooher, *Clinical Trial Lawsuits Are on the Rise*, ST. LOUIS DAILY REC. & ST. LOUIS COUNTIAN, Aug. 31, 2005.

166. See Eliot Marshall, *Shutdown of Research at Duke Sends a Message*, SCIENCEMAG.ORG, <http://www.sciencemag.org/content/284/5418/1246.1.full> (last visited June 6, 2012) (“And with this action—the second shutdown of research at a major clinical center it has ordered in as many months—OPRR has put every federally funded U.S. research institution on notice that its right to conduct clinical research could be summarily yanked.”).

167. See 45 C.F.R. § 46.116 (2011) (“[N]o investigator may involve a human being as a subject in research covered by this policy unless the investigator has obtained the legally effective informed consent of the subject of the subject’s legally authorized representative.”).

168. See *id.* (requiring informed consent for all federally funded research).

169. See Natalie Ram, *Tiered Consent and the Tyranny of Choice*, 48 JURIMETRICS J. 253, 260 (2008) (referring to informed consent as a “term of art”).

170. See Joan H. Krause, *Reconceptualizing Informed Consent in an Era of Health Care Cost Containment*, 85 IOWA L. REV. 261, 361 (2000) (criticizing an approach that “permit[s] patients and physicians to ‘contract out’ of the [informed consent] tort system altogether regarding disclosure obligations” because “it is not clear that [judges] would be free to recognize such a contractual waiver”). Krause goes on to explain that “judicial antipathy to insurers’ ‘medical necessity’ determinations suggests that judges are loathe to enforce insurance contracts where the patient’s health is at stake.” *Id.*

171. See CARL H. COLEMAN ET AL., *THE ETHICS AND REGULATION OF RESEARCH WITH HUMAN SUBJECTS* 297 (2005) (“[As] these two related notions of informed consent have developed, each has been informed by the other . . . In addition, the law governing informed consent to medical care is much better developed than the law governing informed consent to research. Legal principles developed in the context of medical treatment are a useful basis for thinking through some of the unresolved questions in the research setting.”).

research emerge from common values,¹⁷² informed consent to research actually bears the higher burden.¹⁷³

Informed consent to research requires both sufficient procedure and disclosure.¹⁷⁴ The consent must be obtained “under circumstances that provide the prospective subject . . . sufficient opportunity to consider whether or not to participate and that minimize the possibility of coercion or undue influence.”¹⁷⁵ A valid consent form must include the purpose and expected duration of the research; any experimental procedures involved; reasonably foreseeable risks or discomforts to the subject; benefits which may reasonably be expected; appropriate alternative procedures and treatments, if any; the extent to which confidentiality will be maintained; for risky procedures, an explanation of potential compensation and treatments available in case of injury; and who to contact for answers to questions about the study.¹⁷⁶ If children are involved, researchers must provide full information to the child and the child’s parents, and must obtain the child’s assent and the parents’ informed consent.¹⁷⁷

172. See *id.* (acknowledging that informed consent to medical care and research have both been “informed by the other”).

173. See Norman Fost, *Waived Consent for Emergency Research*, 24 AM. J.L. & MED. 163 (1998) (“It has long been accepted that the standards for consent should be higher in the research setting than in ordinary care . . . There are several reasons for this, including the history of serious transgressions, particularly the horrific disclosures of the Nuremberg trials.”).

174. See 45 C.F.R. § 46.116 (2011) (requiring consent “under circumstances that provide the prospective subject . . . sufficient opportunity to consider whether or not to participate” as well as requiring seven basic elements).

175. *Id.*

176. See the Common Rule, *id.* § 46.116(a). Researchers must understand what is meant by “risk” in the Federal Common Rule. Along with the traditional physical harm that medical informed consent was designed to disclose to a patient, informed consent to research includes the various other kinds of harm a subject may experience: emotional, economic, legal liability, etc. Informed consent law is struggling to recognize the wider range of harms that research can inflict upon a human subject. See Cynthia M. Ho, *Who Deserves the Patent Pot of Gold?: An Inquiry into the Proper Inventorship of Patient-Based Discoveries*, 2 HOUS. J. HEALTH L. & POL’Y 107, 121 (2002) (describing typical informed consent as “consent to allow information obtained through the procedure to be used for research purposes, without identification of the individual patient”). Notably, though, informed consent “typically do[es] not indicate that this research may culminate in a patent application . . . [or that subjects] could decline to waive intellectual property rights.” *Id.* at 121–22. Courts are currently struggling with whether the subjects in human subjects research have intellectual property rights in the data collected from them, and if so whether the lack of informed consent can make a researcher liable for the infringement of those rights. See *Greenberg v. Miami Child. Hosp. Res. Inst., Inc.*, 264 F. Supp. 2d 1064 (S.D. Fla. 2003); *Moore v. Regents of the Univ. of Cal.*, 793 P.2d 479 (Cal. 1990); Sharon F. Terry & Patrick F. Terry, *A Consumer Perspective on Forensic DNA Banking*, 34 J. L. MED. & ETHICS 408 (2006). Genetic cell lines have been held patentable. See, e.g., *Diamond v. Chakrabarty*, 447 U.S. 303 (1980); *Amgen Inc. v. Chugai Pharm. Co.*, 927 F.2d 1200 (Fed. Cir. 1991). As the law conferring intellectual property rights on research material develops, informed consent will have to evolve to match it. In the meantime, researchers must be aware of the intellectual property issues as well as the informed consent issues.

177. See 45 C.F.R. § 46.404 (“HHS will conduct or fund research [involving children] only if the IRB finds that adequate provisions are made for soliciting the assent of the children and the permission of their parents or guardians . . .”).

Some virtual worlds researchers—especially those engaged in secondary quantitative research—do not directly obtain informed consent to use a subject's data for research. Instead, these researchers rely on the licensing documents of the game gods,¹⁷⁸ which often merely inform users that their personal and private information may be given to third parties. Yet the legal requirements for consent to human subjects research, described above, are not at all the same as those required for a court to enforce standard terms of online contracts. Courts are often willing to enforce standardized online contracts even though they know that the consumer has likely never read the contract and never considered what the contract contains,¹⁷⁹ which is not the case with consent forms for human subjects research.¹⁸⁰ Commercial contractual consent is a far less stringent standard. Conflating the level of informed consent necessary for human subjects research with that required for online contracts is a common practice but a serious risk.

Most EULAs carefully restrict the ability to withdraw from the agreement. If a user does not consent to all of the terms of the EULA, the user must immediately withdraw from the virtual community.¹⁸¹ Thus, if a user does not consent to the EULA, the result is the loss of the user's online identity and persona, virtual property, social network, and access to the online community. This is an inappropriate procedure for securing consent to human subjects research, which requires that the subject be free to refuse participation, as well as free to withdraw from the research at any time, with no penalty.¹⁸² If a quantitative researcher relies on these restrictive EULAs to substitute for informed consent to human subjects research, the researcher is essentially holding a virtual gun to the subject's head. If the subject does not want information to be used for research

178. See Christina Cary et al., *Data Mining: Consumer Privacy, Ethical Policy, and Systems Development Practice*, 22 HUM. SYS. MGMT. 157, 158 (2003) (“[Companies] assume the users consent to use the information gathered when the user voluntarily uses services that are monitored or fills out a form . . .”).

179. See Ralph James Mooney, *The New Conceptualism in Contract Law*, 74 OR. L. REV. 1131, 1189 (1995) (“Once again [courts] incline strongly toward enforcing contract terms exactly as written, without noticeable regard either for the circumstances surrounding the ‘agreement’ or for its essential fairness. Common examples of such terms being routinely enforced today include arbitration clauses, standardized releases, insurance exclusions, and warranty disclaimers.”).

180. See *The Nuremberg Code*, *supra* note 71 (“The voluntary consent of the human subject is absolutely essential.”). United States courts have recognized that “[t]he universal and fundamental rights of human beings identified by Nuremberg . . . are the direct ancestors of the universal and fundamental norms recognized as *jus cogens*,’ from which no derogation is permitted . . .”). *Abdullahi v. Pfizer, Inc.*, 562 F.3d 163, 179 (2d Cir. 2009) (citing *Sampson v. F.R.G.*, 250 F.3d 1145, 1150 (7th Cir. 2001), and *Siderman de Blake v. Republic of Arg.*, 965 F.2d 699 (9th Cir. 1992)).

181. Most agreements require users to do this by not accessing the virtual world or any websites attached to it, as well as deleting the virtual world software that allows that access.

182. See Sarah Flicker et al., *Ethical Dilemmas in Research on Internet Communities*, 14 QUALITATIVE HEALTH RES. 124, 127 (2004) (allowing nonparticipating subjects to access research site without logging their data, and describing “[c]oercion [as] therefore minimized, as all youth, regardless of research participation, may access the site”).

purposes, the subject's only recourse is to withdraw completely from the virtual world.

Additionally, there is no method for a virtual world participant to opt out of having information used by a researcher after it is gathered by the game god; even if the subject does opt out and ceases all use of the software and attached services, any information collected up to that point generally remains in the data set unless specifically removed by the game god or redacted by the researcher. Researchers may seek to mitigate this problem with secondary data sets by setting up an opt-out site, e-mailing opt-out forms, or by conducting a primary research survey that includes opt-in consent for the secondary data associated with the participant's account. Absent such measures, it is very difficult for a researcher relying on the EULA to provide what the Common Rule requires: adequate assurance to a prospective research subject that there will be no penalty for not participating in the research and the chance to opt out of the use of the subject's data at any time.

The privacy and data protection components of the Common Rule are also related to the autonomy principle. The right to privacy protected by privacy torts—what Justices Warren, Brandeis, and Dean Prosser termed the “right to be let alone”—is closely tied to individual autonomy.¹⁸³ United States courts and legislatures have recognized that autonomy requires a meaningful expectation that one's private information will remain private.¹⁸⁴ In addition to providing participants with adequate information to make important decisions, the informed consent principle operates to protect the privacy of nonparticipants. Researchers should not use private information obtained from nonparticipants because it is outside the scope of informed consent.

For those researchers who seek to log participants' private messages through automated add-on or laboratory video capture of users logged on to their own accounts, there is a real risk that private messages to and from nonparticipant players who have not given consent will be captured, and that harm will result.¹⁸⁵

The problem of capturing nonparticipant communication and conduct arises in both qualitative and quantitative contexts. In the primary qualitative context, researchers may inadvertently observe and record nonparticipant interaction in

183. See M.N.S. SELLERS, *IUS GENTIUM: AN INTRODUCTION TO THE VALUE OF AUTONOMY IN LAW* 2 (2007) (“The importance of autonomy in law is also intimately connected with the concept of privacy . . . ‘Privacy’ is the negative expression of the positive value expressed by ‘autonomy.’ Autonomy signifies the right to decide for oneself. Privacy signifies that zone in which no others may interfere.”).

184. See Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1123–44 (2002) (describing the extant federal and state protections of privacy).

185. As virtual world researcher Lisa Galarneau noted in a 2007 interview:

If it's a private conversation—“tells” or “whispers” versus conversation in a group—it's a *private* conversation. Given the literature around spaces and public conversations etc., I pretty much decided that any conversation I had with anybody where it was very clear it was a private conversation, I would not use even anonymized without explicit consent.

See MCKEE & PORTER, *supra* note 33, at 133 (quoting interview with Lisa Galarneau).

private spaces or contexts, or fail to clearly disclose their research agendas to the community.¹⁸⁶ In the physical world, potential subjects are given warning that they are being observed by the physical trappings of the researcher—including perhaps a tape recorder, a survey clipboard, or a name tag. Users in a virtual world have no way to know that another user may be studying or recording them, absent some signal (such as a guild tag) deliberately created by the researcher. Valid consent in virtual world primary research must be modified to include such signals.

Informed consent to use private messages is complicated in the secondary research context as well. Secondary data sets can include the extremely private conversations of millions¹⁸⁷ of virtual world users over a period of years.¹⁸⁸ These users have not meaningfully consented to the use of their private communications as research fodder, nor would ethical researchers make use of such data since it contravenes the users' expectations of privacy.¹⁸⁹

It is not practical to seek consent for use of stray messages from nonparticipants in a study. Nonparticipants are by definition those who have not given consent to be the subjects of research. Researchers who seek to log players' chat, or lurk and observe their conversations, must either obtain some form of community consent or minimize the danger of capturing nonparticipant private communications. The traditional means of obtaining community consent is to approach a leader of the community, who can grant consent for the community as a whole.¹⁹⁰ Although this latter approach might prove possible in some situations (for example, seeking permission from a guild leader to log guild chat), in general it is not possible to obtain blanket consent from everyone in a virtual world.

Finally, it is useful to note a limiting principle: some chat in virtual worlds is simply not private. Virtual worlds have public places just as the real world does; and a researcher should be able to record public conversations in Stormwind City (a capital city in World of Warcraft) just as she could in a real-world airport or street corner. Knowing the difference is a matter of knowing the world. For this

186. See Frankel & Siang, *supra* note 33, at 11 (“Just as research subjects can be cloaked in anonymity and pseudonymity, so can researchers, raising the issue of deception. Deception occurs when a researcher intentionally misinforms or does not fully disclose relevant information to subjects in cases when informed consent is required.”).

187. See, e.g., William Dobson, *Market Research Firm Predicts Population Explosion for Virtual Worlds*, MASSIVELY (June 16, 2009, 9:00 AM), <http://massively.joystiq.com/2009/06/16/market-research-firm-predicts-population-explosion-for-virtual-w> (explaining that a marketing research firm expected virtual world populations to go from 186.5 million in 2009 to 638 million in 2015).

188. See John Timmer, *supra* note 38 (noting that Sony turned over “the complete server logs from the company’s *Everquest 2* MMORPG” and describing research efforts focused on “interactions like instant messaging, partnerships, and trade”).

189. See Flicker, *supra* note 182, at 128 (“[O]ur position has been that as researchers who are creating sites for research, we are under an ethical obligation to seek consent.”).

190. See, e.g., Elizabeth Reid, *Informed Consent in the Study of On-Line Communities: A Reflection on the Effects of Computer-Mediated Social Research*, 12 INFO. SOC’Y 169 (1996) (securing community leader consent to conduct research in MUDs).

reason, some form of participation in the world by the researcher is a key component of building a research methodology—the researcher must know which spaces (and which chat channels) are considered public by residents, and which are considered private, or limited. Such knowledge would help a researcher understand that broadcast channel chat is almost always public; public chat in public places is nearly certainly public; public chat in private places is probably not public; and so on.

b. Beneficence

The Common Rule demands that researchers minimize the risk of harm to their human subjects.¹⁹¹ Additionally, researchers must ensure that unavoidable risks are “reasonable in relation to anticipated benefits.”¹⁹² Both of these principles are related to *The Belmont Report* principle of beneficence.¹⁹³

Virtual worlds are first and foremost communities. The value players derive from a virtual world emanates from the relationships, friendships, and support they receive from other denizens. The beneficence principle in human subjects research often focuses on avoiding harm to the individual. However, in virtual worlds there is the additional danger that research will harm the individual, both directly and indirectly, through harm to the community. Minimizing harm to the virtual world community is therefore a major focus of virtual world research ethics. Thus, “[virtual world researchers’] main focus of concern [is], first, to protect the entire community (as well as individuals in it) and, second[], not to impair future research(ers).”¹⁹⁴

Bulk logging of private chat for research is questionable not only due to the privacy concerns of the individual, but because it also imposes costs on the entire community. If researchers log private chat messages received by their subjects, the private communications of nonparticipant community members will be swept up in the study. Suddenly, all members must consider whether private communications are being recorded and used for research. This may, in turn, undermine trust and harm the community. The traditional focus of law and ethics on individual consent may cause researchers to overlook detriment to the larger community. McKee and Porter note:

[I]t may be that the risks of a particular study are greater for the community-at-large than to the individual. That is, one participant in a [study] might give permission to have her posts researched and quoted, but in order to obtain those posts the researcher is still engaging or

191. See 45 C.F.R. § 46.111(a)(1) (2011).

192. *Id.* § 46.111(a)(2).

193. See *The Belmont Report*, *supra* note 77 (“Two general rules have been formulated as complementary expressions of beneficent actions in this sense: (1) do not harm and (2) maximize possible benefits and minimize possible harms.”).

194. See MCKEE & PORTER, *supra* note 33, at 120.

lurking within the community Thus, the presence of a researcher or the publicity brought to the group by the reported research may harm the online community.¹⁹⁵

As a result, “[r]esearch may damage communication and community in these forums.”¹⁹⁶

Research can harm virtual communities in other ways as well. Elizabeth Reid has described the effect of her research on one online community in detail.¹⁹⁷ Reid engaged in participant observation of a multi-user dungeon (MUD) community.¹⁹⁸ MUDs are entirely text based and were one of the first types of virtual worlds. Reid obtained specific permission to use all collected data from public Usenet postings,¹⁹⁹ e-mail sent to her,²⁰⁰ and MUD sessions themselves.²⁰¹ She disclosed her status as a recording researcher to the changing population of the MUD.²⁰² But all these precautions focused on the concerns of individual MUD users. Reid still had to grapple with her ethical obligations to the community as a whole:

I decided to contact the administrators of each MUD I used, tell them about my research, assure them that I would ask permission of each individual to quote material, and ask for permission to discuss their MUD in my thesis. This decision involved an assumption that a MUD’s administrator was in a position to speak for the MUD community as a whole. At the time this seemed a sensible assumption, and one that seemed to be shared by both the administrators and the users.²⁰³

Many communities and administrators welcomed Reid with open arms.²⁰⁴

195. *Id.* at 33 (citations omitted).

196. *See* Gunther Eysenbach & James E. Till, *Ethical Issues in Qualitative Research on Internet Communities*, 323 *BRIT. MED. J.* 1103, 1104 (2001) (quoting one study participant who dropped out of an online support group, noting, “‘When I joined this, I thought it would be a support group, not a fishbowl for a bunch of guinea pigs. I certainly don’t feel at this point that it is a safe environment’”).

197. *See* Reid, *supra* note 190.

198. *See id.* at 169 (noting that she participated in the MUD for two years).

199. *Id.* at 169–70. Despite her belief that “the author [of the Usenet articles] could not reasonably expect to exclude any person from gaining access to his or her words,” Reid felt that “[i]n the absence of clearly defined legal or cultural specifications regarding the use of material distributed via Usenet [it would be] best to take the more cautious—and courteous—path of asking each author’s individual permission to include their material in [her] thesis.” *Id.*

200. *See id.* at 170. (“In the case of email it seemed clear that since [Reid] was the only intended recipient [she] should seek permission before including such material.”).

201. *See id.* (“[B]efore referring to individuals or quoting from conversations and environment descriptions in [her] thesis [Reid] asked for permission from those concerned to do so.”).

202. *Id.* (using “a virtual approximation of a visible tape recorder: [her] MUD characters’ personal descriptions included mention of a tape recorder, notebook, or other device suitable to the particular milieu of the MUD”).

203. *Id.* at 170–71.

204. *See id.* at 171–72 (“Not once was [she] refused permission by either MUD players of administrators to include them in [her] work.”). In fact, Reid “was also subject to the phenomenon of people who on learning the nature of [her] research set about to deliberately manufacture quotable quotes” *Id.*

However, “[i]n at least one case [her research had] a negative effect on its subjects.”²⁰⁵ Reid describes her “discomfort[] in the eagerness with which MUD users seemed to embrace the opportunity to be a research subject.”²⁰⁶ Because of this discomfort, she did not “publish[] extracts from e-mail and MUD session logs that revealed deeply personal information about these people’s lives and experiences,” even though her informed consent forms gave her the right to do so.²⁰⁷ Even with the additional restrictions on information about the MUD, Reid received many requests for information about the MUD after publication of her thesis.²⁰⁸ She forwarded some requests to the leader of the MUD, but eventually the influx contributed to significant harm to the MUD community:

The MUD had reached a crisis point. Where a feeling of safety and privacy had reigned there now existed distrust and wariness. Users were connecting to the MUD with declining frequency, and the social networks and alliances that had flourished on it showed signs of strain. In order to protect and consolidate this small virtual society, [the leader] had decided to batten down the hatches and increase security on the MUD [The leader] and I both came to the conclusion that this uncomfortable stage in the MUD’s development might have been quickly overcome had it not been for the decision to invite further public scrutiny and personal exposure through participation in my research project.²⁰⁹

Reid concludes that she underestimated the “disinhibiting effect of computer-mediated communication.”²¹⁰ She warns that “the experience of scrutiny inherent in being involved in a research project may itself be damaging,”²¹¹ and laments her own involvement in changes to the MUD:

[The leader] no longer advertises the MUD in various mailing lists and Usenet groups. New members are now attracted only through discreet word of mouth, and must be sponsored and vouched for by an existing member. Internal constraints on the building and programming abilities of members have been instituted. Members are no longer able to use the command that allows messages to be sent simultaneously to all others logged on at any given time. These measures have made the MUD safer and less open [E]vents have forced the members of the system to trade “freedom to” for “freedom from”—a trade-off I regret having been a factor in necessitating.²¹²

205. *Id.*

206. *Id.* at 172.

207. *Id.*

208. *See id.* Some “expressed an interest in joining the MUD for personal reasons,” and “a significant number came from a variety of social scientists who wished to conduct further studies.” *Id.*

209. *Id.*

210. *Id.*

211. *Id.*

212. *Id.* at 173.

These are not problems that traditional informed consent was designed to solve.²¹³ Researchers should account for the communal nature of virtual worlds. They should take precautions to safeguard the community as a whole, in addition to those individuals directly participating in the research. And, even if researchers take all available precautions, some harm may still result to the community due to the research. This risk does not prohibit researchers from conducting studies in virtual worlds. Rather, the beneficence principle requires researchers to be aware of potential risks, to minimize those risks they can, and to be sure that any remaining risk is proportional to the possible benefits.²¹⁴

c. Justice

The Belmont Report requires researchers to equitably distribute the benefits of research.²¹⁵ By choosing research subjects fairly, researchers can ensure that the research benefits are distributed equally.²¹⁶ The Common Rule also encourages equitable selection of subjects.²¹⁷ *The Belmont Report* and the Common Rule discourage subject selection based solely on subject availability.²¹⁸ Virtual worlds may pose challenges under the justice principle because they are demographically limited and the results of any research would be similarly limited.

It is important not to overstate the issue. Human subjects research is conducted on narrow population segments all the time. For example, genetic studies regularly relate solely to the groups that contain specific genes.²¹⁹ Psychological experiments are often conducted on college students, since college students seem to be broadly available and have free time that they are willing to exchange for small payments.²²⁰ Similar attributes of virtual worlds studies are

213. *Id.* (“The criteria for informed consent that may be sufficient in face-to-face research environments are not necessarily enough in a medium in which subjective experience is easily objectified and information easily devalued.”).

214. *See The Belmont Report, supra* note 77.

215. *See The Belmont Report, supra* note 77 (“[W]henver research supported by public funds leads to the development of therapeutic devices and procedures, justice demands both that these not provide advantages only to those who can afford them and that such research should not unduly involve persons from groups unlikely to be among the beneficiaries of subsequent applications of the research.”).

216. *See The Belmont Report, supra* note 77 (“[T]he selection of research subjects needs to be scrutinized in order to determine whether some classes . . . are being systematically selected simply because of their easy availability, their compromised position, or their manipulability, rather than for reasons directly related to the problem being studied.”).

217. *See* 45 C.F.R. § 46.111(a)(3) (2011) (requiring equitable selection of subjects as a condition of IRB approval).

218. *See* Greely, *supra* note 86 and accompanying text.

219. *See, e.g.,* UCSD Dep’t of Psychiatry Genetics Research Program, *Bipolar Research*, UCSD, <http://www.bipolar.ucsd.edu/BPResearch.htm> (last visited June 6, 2012) (requesting volunteers for genetic bipolar research and requiring determination of eligibility based on family history of bipolarity).

220. *See, e.g., Interested in Participating in a Psychology Experiment?*, DARTMOUTH, <http://www.dartmouth.edu/~psych/experiments> (last visited June 6, 2012) (offering experiment participation

likely not of concern. The fact that virtual world participants tend to be college-aged and older seems to cause no imbalance that is broadly problematic among researchers.²²¹ However, it may be useful for researchers, IRBs, and funding agencies to broaden the range of virtual worlds studied in order to study a range of demographics.²²² Current virtual world demographics probably satisfy the justice requirement of *The Belmont Report* and its associated regulations—but that fact does not preclude conscientious researchers from improving their practices through greater inclusiveness.

Perhaps a more discomfiting concern is that of the digital divide. Although it is possible to find virtual worlds that cater to different age and gender demographics, it is not possible to find a virtual world that caters to people without access to the requisite computing technology. Both high-end video cards and fairly high bandwidth are necessary components for participation in many virtual worlds.²²³ Thus, populations without access to good computers or bandwidth—such as underprivileged households or rural populations—will not benefit from virtual worlds research.

There is reason to believe that these effects will be ameliorated by trends already observable in technology and the literature. Virtual worlds are moving toward less-intensive graphics and greater participation.²²⁴ Two-dimensional, isometric, and Flash virtual worlds are emerging very rapidly; the flashier and more graphics-intensive virtual worlds are growing at a slower rate. The fastest-growing virtual worlds are those like Club Penguin that can be run from within a browser.²²⁵ Simpler virtual worlds require less bandwidth overall; some require no

opportunities to students); *Psychology, Research Opportunities*, AM. U., <http://www.american.edu/cas/psychology/resources/opportunities.cfm> (last visited June 6, 2012) (same); *Sign Up for Studies*, HARVARD U., <http://studypool.wjh.harvard.edu/SignUp.html> (last visited June 6, 2012) (same).

221. See *The Belmont Report*, *supra* note 77 (“Almost all commentators allow that distinctions based on experience, age, deprivation, competence, merit and position do sometimes constitute criteria justifying differential treatment for certain purposes.”).

222. See discussion *infra* Part IV.G (discussing best practices for diversifying virtual worlds research).

223. See, e.g., *Minimum System Requirements for World of Warcraft*, BLIZZARD, http://us.blizzard.com/support/article.xml?locale=en_US&articleId=21054 (last visited June 6, 2012) (describing the system requirements for World of Warcraft); *System Requirements*, SECOND LIFE, <http://secondlife.com/support/system-requirements> (last visited June 20, 2010) (same); *PlayOnline & Final Fantasy XI for Windows System Requirements*, PLAYONLINE (Oct. 2009), <http://www.playonline.com/ff11us/envi/win/win01.html?pageID=win> (describing system requirements for play and observing that “[a]pplication performance is highly dependent on the type of hardware and Internet connection speeds”).

224. See discussion *supra* Part II.

225. See Sabitri Ghosh, *The \$350 Million Penguin*, GLOBE & MAIL (Nov. 18, 2009), <http://www.theglobemail.com/report-on-business/small-business/exit/selling-your-business/article1368439.ece> (noting that “Club Penguin’s registered users . . . leapt to 28 million by [Summer 2008]” and that in summer 2007 there were “12 million registered users”).

more than a regular website.²²⁶ Similarly, there is some hope that populations that have not previously had access to broadband will be able to participate in virtual worlds with the rollout of 4G data networks and municipal Wi-Fi.²²⁷

d. Special Protections for Minors in Virtual Worlds

The Common Rule provides additional protection for vulnerable populations, including minors, pregnant women, and incarcerated persons.²²⁸ Because so many children play in virtual worlds, this Section will focus on the challenges posed by minors in virtual world studies. No virtual worlds study to date has made use of incarcerated persons, nor have the studies adopted methodologies that impact pregnant women.

In the special case of minor human subjects, there are two broad concerns. First, research that poses more than a minimal risk to a minor must provide a direct benefit.²²⁹ Second, the Common Rule imposes additional and heightened consent requirements—both the child and the child’s parents must be informed and must consent to the research.²³⁰

Subpart D of the Common Rule requires that research posing more than minimal risk to the minor participants must provide a direct benefit to the particular minor human subjects engaged in the study.²³¹ The general social benefits that scientific research confers do not satisfy the direct benefit requirement.²³² Primary methodologies allow researchers to satisfy this requirement by providing a benefit at the time of information collection.²³³ Secondary quantitative methodology makes compliance with this standard very difficult. In secondary quantitative methodologies, the researcher never engages the human subject.²³⁴ Instead, the data is often gathered by the game gods for

226. Compare *Minimum System Requirements for World of Warcraft*, *supra* note 223 (requiring broadband connection), with *I Need to Know How Fast My Connection Should Be?*, SUPPORT.CLUBPENGUIN, http://support.clubpenguin.com/help/technical/connection_how_fast.htm (last visited June 6, 2012) (“Club Penguin is designed to work with a 56 K modem or higher.”).

227. See Mark G. Tratos, *The Continued Evolution of Standard Terms in Database Licensing Agreements*, in 995 PLI/PAT 873, 877 (2010) (“[T]he rise of new networks such as broadband, Wi-Fi, 3G and 4G have increased the demand for instant access to data.”).

228. See 45 C.F.R. §§ 46.201–.207, .301–.303, .401–.409 (2010).

229. See *id.* § 46.405.

230. See *id.*; see also *id.* § 46.408.

231. See *id.* § 46.405.

232. See *id.* There is, however, one exception in the Federal Common Rule requirements for direct benefit: research involving minor participants that is not otherwise approvable, but which “presents an opportunity to understand, prevent, or alleviate a serious problem affecting the health or welfare of children” may be conducted if additional requirements are met. *Id.* § 46.407. The additional requirements relate to the approval by the IRB and the Secretary. See *id.*

233. For example, a study on Internet behavior on children might be accompanied by an Internet citizenship course teaching children how to behave online.

234. See discussion *supra* Part III.A.1 (discussing secondary research).

commercial purposes.²³⁵ Thus, a minor subject whose information is analyzed in this manner cannot receive the required direct benefit at the time of information collection.

The heightened consent requirements for children can also be difficult to meet in an online environment. Primary qualitative researchers regularly work with children in virtual worlds because they can meet with the minor participant and secure informed consent from the minor and the minor's parents. However, researchers who only interact with research subjects online often attempt to exclude minors from their research protocols, IRB submissions, and studies altogether.

It is particularly difficult to exclude minors from secondary commercial data sets. Game gods record almost everything that occurs in virtual worlds, from chat logs to economic transactions.²³⁶ The data sets include all users of the virtual world, and inevitably there are minor users. While many virtual world providers seek to exclude children under thirteen from accessing the world because of the requirements of the Children's Online Privacy Protection Act,²³⁷ these methods are not foolproof. Children can and do access virtual worlds by lying about their ages, and children over the age of thirteen are not excluded.²³⁸

Moreover, the age of exclusion is different for commercial entities than it is for researchers bound by the Common Rule. The Common Rule requires that researchers exclude children who are below the age of consent for the area in which the research is being conducted.²³⁹ Children access virtual worlds from across the United States and throughout the world. Thus, determining the age of consent for children whose data is captured in a virtual world is impracticable at

235. This recording serves different commercial purposes; chat logging, for example, assists with customer service disputes, while logging of economic transactions permits the game gods to protect the money supply against virtual counterfeiters.

236. See *Privacy Policy*, SECOND LIFE, <http://secondlife.com/corporate/privacy.php#privacy1> (last revised Oct. 11, 2011) [hereinafter *Second Life Privacy Policy*] ("We collect a range of personal information and usage statistics . . . We request some information directly from you during registration. We gather other pieces of data indirectly from Website traffic, your computer hardware and Internet connection, or your Second Life activities, communications and usage.").

237. 15 U.S.C. §§ 6501–6505 (2006). These requirements, discussed *infra* Part III.B.3.b, can be burdensome; to avoid them, game gods typically exclude children who fall in COPPA's twelve-and-under threshold of eligibility.

238. See FED. TRADE COMM'N, VIRTUAL WORLDS AND KIDS: MAPPING THE RISKS 14 (2009) ("Of the seven online virtual worlds that set a minimum participation age of 13, all rejected attempts to register below that age. However, two worlds, Kaneva and There.com, rejected child registrations, but then immediately permitted users to re-register as an adult from the same computer . . . Another five worlds disallowed underage registrations, and then took the additional step of rejecting immediate attempts to re-register as age-eligible users from the same computer."). The FTC went on to conclude: "Although some of the teen- and adult-oriented online virtual worlds . . . have taken steps to restrict minors' access . . . their efforts have not fully succeeded." *Id.* at 19.

239. See 45 C.F.R. § 46.40(a) (2011) ("*Children* are persons who have not attained the legal age for consent . . . under the applicable law of the jurisdiction in which the research will be conducted.").

best. Even in the United States, the age of consent can vary—usually between sixteen and eighteen. The global nature of many virtual worlds makes the age of consent calculus even more erratic. Researchers who receive full data sets from game gods can be certain that enormous amounts of personal information collected from fourteen- to seventeen-year-olds will be included in the data set.

Primary qualitative researchers can effectively exclude children by meeting the research subjects in person or by requiring other verification of age before beginning ethnographic studies. A secondary qualitative researcher can limit research to data sets for which the primary researcher verified the subjects' ages. However, a quantitative researcher faced with several terabytes of data gathered by the game gods will simply not be able to ensure that children are excluded. While a secondary quantitative researcher may not be able to completely eliminate this risk, best practices (as discussed below) will permit the researcher to minimize it.

e. The Advance Notice of Proposed Rulemaking (ANPRM)

In 2011 the Office of the Secretary of the Department of Health and Human Services issued an advance notice of proposed rulemaking (ANPRM) that would significantly reform the Common Rule.²⁴⁰ Although these proposals are not finalized, it is useful to address the proposed changes and the impact they may have on the analysis presented here. My conclusion is that although the proposed changes lighten the load on researchers during the research phase,²⁴¹ they broaden the scope of the rule to include research not previously covered²⁴² and impose heightened requirements on researchers at the front end, that is, at the time that data is gathered (in the form of enhanced consent requirements),²⁴³ and at the back end, that is, after the data is gathered, by imposing mandatory data protection standards.²⁴⁴

240. Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. 44,512 (July 26, 2011) (to be codified at 45 C.F.R. pt. 46, 160, and 164, and 21 C.F.R. pt. 50 and 56). (“[D]ecades of experience have revealed a great deal about the functioning—and limitations—of existing regulations Addressing these considerations now is timely”) *Id.* at 44,513.

241. *Id.* at 44,515 (“Continuing review would be eliminated for all minimal risk studies that undergo expedited review . . . [and the revised] regulations regarding expedited review . . . [would] creat[e] a presumption that studies utilizing only research activities that appear on [the expedited review list] are indeed minimal risk, and providing for streamlined document submission requirements for review.”); *id.* at 44,516 (“Standardized data protections, rather than IRB review, may be a more effective way to minimize informational risks.”).

242. *Id.* at 44,514 (“Extension of Federal regulatory protections to all research, regardless of funding source, conducted at institutions in the U.S. that receive some Federal funding from a Common Rule agency for research with human subjects.”).

243. *Id.* at 44,523 (“We are considering a number of modifications to the regulations to improve consent forms”).

244. *Id.* at 44,525 (“[A] solution we are considering is to mandate data security and information protection standards that would apply to all research that collected, stored, analyzed or otherwise reused identifiable or potentially identifiable information.”).

The current definition of human subjects research depends on two terms: “research” and “human subjects.” The Common Rule defines research as “a systematic investigation,”²⁴⁵ and human subjects as subjects with whom the researcher has interacted,²⁴⁶ or from whom the researcher has obtained identifiable private information.²⁴⁷ “Exempt” research did not need to comply with the Common Rule’s requirements;²⁴⁸ nonexempt research was required to do so.²⁴⁹ The question of whether research fell under the Common Rule or not was therefore of significant importance.

The proposed changes shifted the focus from whether or not the research fell under the definition of human subjects research²⁵⁰ and instead moved toward a broad-based requirement that all research conducted by an organization that received federal funding would be subject to the requirements of the new Common Rule.²⁵¹ All research falling under the new definition would be subject to the Common Rule’s requirements, for example, for consent or heightened data protection. An IRB would not be required to pass on proposals that do not present serious risks. The ANPRM proposes a new category: research that falls under the expanded ambit of the Common Rule but does not trigger the requirement that an IRB review the research protocols would be termed “excused” rather than “exempt.”²⁵²

This new category of “excused” research may well include many of the methodologies used to study virtual worlds. For example, survey methods, interviewing, and other standard techniques common in the behavioral and social sciences would fall into this category.²⁵³ (The precise techniques excused are still in debate as part of the rulemaking process, which also proposes to regularly update the list of excused techniques.) In addition, the proposed changes directly address the question of data gathered for nonresearch purposes and resolve much

245. 45 C.F.R. § 46.102(d) (2011).

246. *Id.* § 46.102(f)(1).

247. *Id.* § 46.102(f)(2).

248. *Id.* § 46.101(b) (“Unless otherwise required by department or agency heads, research activities in which the only involvement of human subjects will be in one or more of the following categories are exempt from this policy.”).

249. *Id.* § 46.101(a) (“Except as provided in paragraph (b) of this section, this policy applies to all research involving human subjects . . .”).

250. *Id.* § 46.102(d), (f).

251. Human Subjects Research Protections, *supra* note 240, at 44,528 (“We are considering . . . requiring domestic institutions that receive some Federal funding from a Common Rule agency . . . to extend the Common Rule protections to all research studies conducted at their institution.”).

252. *Id.* at 44,518 (“We are considering revising the category of exempt research . . . Given that these studies would no longer be fully exempt from the regulations, they could more accurately be described as ‘Excused’ from being required to undergo some form of IRB review . . .”).

253. *Id.* at 44,518 (“[R]esearch conducted with competent adults, that involve educational tests, surveys, focus groups, interviews, and similar procedures would qualify for the new Excused category . . .”).

ambiguity in the treatment of these data sets by drawing them directly under the ambit of the proposed new Rule.²⁵⁴

However, the fact that much of virtual worlds research would either qualify as excused or for reduced requirements (since the risk of harm is often minimal) does not relieve virtual worlds researchers of the need to pay attention to the law of human subjects research. Indeed, virtual world researchers must pay more attention, since research that was previously “exempt” from the Rule would be covered by the expanded rule, even if such research fell into the new “excused” category. The heightened consent and data protection requirements free researchers to gather and retain private and identifiable information²⁵⁵—but the stress falls on these heightened front- and back-end requirements.

Of particular interest are the proposed clarifications to the use of data sets that were originally gathered for nonresearch purposes. As this Article has previously noted, game gods gather colossal data sets on everything that the users of virtual worlds do, from their intimate conversations to their economic transactions. The circumstances under which this data would become available to researchers is of significant importance to companies that gain from scientific analysis of the data sets they have gathered and researchers who benefit from complete data sets covering many users over a period of years.

The proposed revised treatment of secondary data sets would clarify the law’s treatment of such data; data gathered for nonresearch purposes would be permissible, but subject to a written consent requirement if the data contains individually identifiable information.²⁵⁶ Interestingly, the ANPRM contemplates that written consent for research use would be obtained at the time of the collection of the data.²⁵⁷ This requirement may be an artifact of the drafting of the rules from the biomedical perspective. In the medical context, it is not strange to assume that consent for research use of samples gathered for nonresearch purposes might be secured at the time the sample was taken. But for large commercial data sets, the enhanced written consent requirements seem a bit odd. The proposed changes would require companies to put clauses in their EULAs or

254. *Id.* at 44,525 (“[A] solution we are considering is to mandate data security and information protection standards that would apply to all research that collected, stored, analyzed or otherwise reused identifiable or potentially identifiable information. This would include . . . secondary analysis of the data.”).

255. *See* Human Subjects Research Protections, *supra* note 240, at 44,523–24.

256. *Compare id.* at 44,519 (“If the data was originally collected for non-research purposes, then, as is currently the rule, written consent would only be required if the researcher obtains information that identifies the subjects.”), *with id.* at 44,525 (“We are considering adopting the HIPAA standards for purposes of the Common Rule.”), which effectively updates the current rule, *and id.* at 44,524 (“The HIPAA Privacy and Security Rules generally require safeguards for individually identifiable health information and place limits and conditions on the use and disclosure of such information.”).

257. *Id.* at 44,524 (“The assurance that identifiable information will be safeguarded is important for an individual’s willingness to participate in research.”).

TOSs that would clearly contemplate the use of data for research purposes even though the data was being gathered for nonresearch (i.e., customer demographics or targeted advertising) purposes. This creates something of a contradiction. Data gathered “not for research purposes” must nevertheless be gathered subject to contractual conditions that contemplate research in order for the data to be used for research down the line.

Under the proposed changes, companies would be wise to include consent clauses in their EULAs or TOSs that secure consent for research use of the data. But this is not all. The consent obtained may also need to comply with the proposed changes’ enhanced clarity and simplicity requirements.²⁵⁸ Whether this means that EULAs must use language set out by the Common Rule in order to later use data for research purposes is not clear from the ANPRM. One element that is clear, and is of special note to virtual worlds researchers, is that the ANPRM clearly contemplates consent as being valid only if it can be meaningfully refused. Thus, the ANPRM states: “Importantly, this standardized general consent form would permit the subject to say no to all future research.”²⁵⁹ That is, the subject could say no to research but still obtain medical treatment. But there is no such option in the collection of large commercial data sets. Consumers cannot refuse the EULA and still use the service.

The problem with commercial data sets gleaned from virtual worlds should be obvious. These contracts are consumer contracts of adhesion, regularly modified at the whim of the game god. The user is never presented a meaningful option to refuse consent: if the user does not wish to abide by the terms that the game god offers, the user may choose not to enter the virtual world. If a game god were to alter its EULA or TOS to include the kind of general standardized consent to human subjects research that the ANPRM contemplates, the user would not have a meaningful opportunity to decline. The user would have to either agree to the changed EULA or give up all of his or her online community, property, and account progress. In short, the subject’s attachment to the virtual world would be held hostage by the researcher. As noted above, this cannot be the kind of free-willed declinable consent that the Common Rule or the ANPRM contemplates.

The ANPRM permits researchers to obtain and retain identifiable private information as long as researchers comply with its heightened consent requirements and data security requirements. Further, many categories of social science will be exempt if the ANPRM’s proposals are carried out, and even those experiments that are not will benefit from a default presumption of expedited

258. *Id.* at 44,523 (“We are considering a number of modifications to the regulations to improve consent forms, including . . . limiting the acceptable length of various sections of a consent form . . . [and] reducing institutional ‘boilerplate’ in consent forms.”).

259. *Id.* at 44,519 (“Importantly, this standardized general consent form would permit the subject to say no to all future research.”).

review as minimal risk studies.²⁶⁰ For virtual worlds researchers conducting primary research, this means that the bulk of the responsibility for determining the risk of a study falls on the researcher rather than on an IRB. The researcher would make the determination as to whether the study was excused or expedited, and would in fact be free to begin research upon filing the appropriate declaration.²⁶¹

But the ANPRM's proposed changes, especially those requiring written consent for the use of identifiable information gathered for nonresearch purposes,²⁶² fit very poorly with secondary research on large commercial databases. The ANPRM requirements of simplified consent do not square with industry practice in drafting endless and incomprehensible EULAs. Nor would the addition of a simplified consent clause simplify the overall document—a generalized research consent clause would be merely another EULA clause that the consumer does not read.

If the ANPRM's proposals are adopted, researchers on large commercial data sets gathered on massive online communities should do one of three things. First, researchers should, when possible, work from de-identified data sets, with avatar names and guild designations removed. This moves researchers away from the requirement of written consent and toward the ANPRM's more lenient notion of general oral consent given at the time of the collection of the information.²⁶³ Second, if a researcher must receive identifiable data from a commercial entity, the researcher might secure consent by conducting separate primary research that secures written consent from the survey participants for use of their secondary data. Thus, for example, a virtual worlds researcher who has a large secondary data set might seek study participants online and only use the secondary data of those users who directly grant consent as part of the researcher's primary research. Third, the researcher could work with the game god to secure the ANPRM's proposed generalized, standardized, simple, and meaningfully refusible consent to the research use of the data. The difficulty is that this option runs directly against industry practice (especially as regards meaningful refusal), and would very much complicate the relationship between researcher and commercial entity. It is already hard enough to build bridges from academia to business. This additional requirement will likely stifle any collaboration.

260. *Id.* at 44,516 (“We are accordingly considering providing a default presumption in the regulations that a study which includes only activities on the list is a minimal risk study and should receive expedited review.”).

261. *Id.* at 44,515 (“Require that researchers file with the IRB a brief form . . . to register their exempt studies, but generally allow the research to commence after the filing . . .”).

262. *See supra* note 240 and accompanying text.

263. *Id.* at 44,520 (“[O]n those occasions when oral consent was acceptable under the regulations for the initial data collection, it is envisioned that subjects would have typically provided their oral consent for future research at the time of the initial data collection; a written consent form would not have to be signed in that circumstance.”).

2. *Copyright and Terms of Service/End User License Agreement*

Recording is what researchers do. But “[q]uestions of intellectual property arise whenever a researcher . . . quotes excerpts from subjects’ writings, or captures screen shots of their web sites, or reproduces their avatar from *Second Life* or their game character from *World of Warcraft*.”²⁶⁴ Recording within a virtual world raises complicated legal issues because every object, avatar, and location within a virtual world must be licensed to be lawfully recorded.

The collection of data is pivotal to successful research, and as a result researchers have developed diverse tools to help them collect data in virtual worlds. This subpart discusses the law’s treatment of some of the most common methods of recording data within virtual worlds.

One common tool is the “add-on,” a bit of software used by a player within a virtual world that interacts with the virtual world program as part of the player’s user interface.²⁶⁵ Another tool is the use of screen-capture software that records everything that happens on-screen.²⁶⁶ Researchers also use “bots” or “scrapers”—computer programs that search a target website or virtual world and record the data found there.²⁶⁷ A somewhat more primitive recording device is the placement of a physical video camera facing a monitor while in-world actions take place.²⁶⁸ Copyright and licensing issues are involved in all of these data recording methods.²⁶⁹

a. *Copyright in Virtual Worlds*

Copyright infuses virtual worlds. Every object, avatar, texture, conversation, and place in a virtual world is copyrighted.²⁷⁰ These copyrights generally belong to

264. MCKEE & PORTER, *supra* note 33, at 56.

265. See *AddOn*, WOWWIKI, <http://www.wowwiki.com/AddOn> (last visited June 6, 2012) (“AddOns are generally self-contained User Interface (UI) modification components . . . In plain English, an AddOn is just some files you can put in your game folder that can (theoretically) improve your interaction with the World of Warcraft game (i.e. make it easier to play, or give you more information about what’s going on in the game).”).

266. See, e.g., *Quick Screen Capture*, ETRUSOFT, <http://www.etrusoft.com> (last visited June 6, 2012) (an example of screen-capture software); *CamStudio Open Source*, CAMSTUDIO.ORG, <http://camstudio.org> (last visited June 6, 2012) (same); *ALL.Capture*, BALEGIO, <http://www.allcapture.com/eng/index.php> (last visited June 6, 2012) (same).

267. See *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058, 1060–61 (N.D. Cal. 2000) (“A software robot is a computer program which operates across the Internet to perform searching, copying and retrieving functions on the web sites of others. A software robot is capable of executing thousands of instructions per minute, far in excess of what a human can accomplish.”).

268. See *infra* Part III.B.2.c.

269. See *infra* Part III.B.2.c.

270. See *Terms of Use*, WORLD WARCRAFT, http://www.worldofwarcraft.com/legal/terms_of_use.html (last visited June 6, 2012) [hereinafter *World of Warcraft Terms of Use*] (“All rights and title in and to the Service (including without limitation any user accounts, titles, computer code, themes, objects, characters, character names, stories, dialogue, catch phrases, locations, concepts, artwork, animations, sounds, musical compositions, audio-visual effects, methods of operation, moral rights,

the game god, which uses the EULA to turn its ownership of copyright in the basic structures, textures, and effects of the game into ownership of everything the players do in the game.²⁷¹ In the physical world the objects, places, and people that researchers observe are not copyrighted.²⁷² In virtual worlds, however, every aspect of the world has been consciously created and fixed in the virtual medium by someone. Everything researchers observe in a virtual world is subject to copyright—by the player, if the game EULA permits players to retain intellectual property rights, or by the game gods, either directly or through the player's contractual assignment of all rights.²⁷³ Thus, conducting research in a virtual world almost inevitably means making copies of protected intellectual property, whether in the form of images or text. Because almost all chat is stored on game servers,²⁷⁴ even recording player chat raises copyright issues.

The Digital Millennium Copyright Act (DMCA)²⁷⁵ further complicates copyright law in virtual worlds. In the offline world, the cost and inconvenience of making numerous copies of someone else's physical intellectual property serve as

any related documentation, 'applets,' transcripts of the chat rooms, character profile information, recordings of games) are owned by Blizzard or its licensors."); *see also Second Life Privacy Policy*, *supra* note 236 ("You retain any and all intellectual property rights you already hold under applicable law in Content you upload, publish, and submit to or through the Servers, Websites, and other areas of the Service, subject to the rights, licenses, and other terms of this Agreement, including any underlying rights of other users or Linden Lab in Content that you may use or modify.").

271. *See End User License Agreement*, WORLD WARCRAFT, <http://www.worldofwarcraft.com/legal/eula.html> (last visited June 6, 2012) [hereinafter *World of Warcraft End User License Agreement*] ("All title, ownership rights and intellectual property rights in and to the Game and all copies thereof (including without limitation any titles, computer code, themes, objects, characters, character names, stories, dialog, catch phrases, locations, concepts, artwork, character inventories, structural or landscape designs, animations, sounds, musical compositions and recordings, audio-visual effects, storylines, character likenesses, methods of operation, moral rights, and any related documentation) are owned or licensed by Blizzard."); *see also World of Warcraft Terms of Use*, *supra* note 270 ("All rights and title in and to the Service (including without limitation any user accounts, titles, computer code, themes, objects, characters, character names, stories, dialogue, catch phrases, locations, concepts, artwork, animations, sounds, musical compositions, audio-visual effects, methods of operation, moral rights, any related documentation, 'applets,' transcripts of the chat rooms, character profile information, recordings of games) are owned by Blizzard or its licensors.").

272. *See Fritz v. Arthur D. Little, Inc.*, 944 F. Supp. 95, 100 (D. Mass. 1996) ("If true, th[e] claim that the source of the allegedly infringing materials was not 'fixed in any tangible medium of expression' when copied would defeat Fritz's claim of copyright infringement. 'Original' words spoken aloud can be copied (and independently copyrighted) by all, if they have not previously been fixed in a tangible medium of expression.") (quoting *Bleistein v. Donaldson Lithographing Co.*, 188 U.S. 239, 249 (1903)).

273. *See, e.g., World of Warcraft Terms of Use*, *supra* note 270 (assigning ownership of in-world content).

274. *See id.* (including "dialogue" and "transcripts of the chat rooms" in data owned by Blizzard Entertainment); *Second Life Privacy Policy*, *supra* note 236 ("We may collect and retain any other information relating to your account data or in-world activities including chat or IM logs . . .").

275. 17 U.S.C. §§ 512, 1201–1205, 1301–1332 (2006).

discouraging factors;²⁷⁶ in the digital context, however, copies can be made instantaneously, easily, and with almost no cost to the copier.²⁷⁷

Digital intellectual property owners have thus used technological measures—including the mandatory clickthrough licensing agreements that govern most virtual worlds to restrict copying of digital content.²⁷⁸ The DMCA makes circumventing these technological measures unlawful.²⁷⁹ Almost all virtual worlds have mandatory clickthrough EULAs that courts have deemed to serve as technological measures controlling access and use of the software.²⁸⁰ A researcher therefore faces a catch-22. If the researcher refuses to click through the EULA and instead hacks the software to gain access, the DMCA imposes liability for circumventing access controls to copyrighted material.²⁸¹ If the researcher clicks through the EULA, the researcher may give up some fair use rights (as discussed below).²⁸² Thus, the DMCA forces anyone who accesses the software to agree to the EULA. The EULA, in turn, may contain various waivers of fair use rights.²⁸³ The fair use defense is thus of quite limited use in virtual worlds. Rather, the terms of the EULA dictate what a researcher can do.

Even worlds that permit players to own their user-generated content pose serious copyright concerns to researchers. In *Second Life*, players retain ownership of the avatars, objects, and structures they design within the world.²⁸⁴

276. See H.R. REP. NO. 105-551, pt. 2, at 25 (1998) (“In contrast to the analog experience, digital technology enables pirates to reproduce and distribute perfect copies of works—at virtually no cost at all to the pirate.”).

277. *Id.*

278. See, e.g., *World of Warcraft Terms of Use*, *supra* note 270 (“Your use of the Game Client is subject to the World of Warcraft End User License Agreement (the ‘EULA’). Your use of the Service is subject to this Terms of Use . . . You must accept the EULA, the Terms of Use . . . prior to playing the Game.”); *Second Life Terms of Service*, *supra* note 39 (“By using Second Life, you agree to and accept these Terms of Service. If you do not so agree, you should decline this Agreement, in which case you are prohibited from accessing or using Second Life.”).

279. See 17 U.S.C. § 1201(a)(1)(A) (2006) (“No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”).

280. See Timothy K. Armstrong, *Fair Circumvention*, 74 BROOK. L. REV. 1, 3 (2008) (“Although the statute states Congress’s intention to preserve fair use, the anti-circumvention provisions of the DMCA make no express exceptions for fair uses, and some courts have rejected the notion that a party accused of a DMCA violation may interpose a fair use defense.”).

281. U.S. COPYRIGHT OFFICE, THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, at 4 (1998), available at <http://www.copyright.gov/legislation/dmca.pdf> (“[S]ince the fair use doctrine is not a defense to the act of gaining unauthorized access to a work, the act of circumventing a technological measure in order to gain access is prohibited.”).

282. See *Davidson & Assocs. V. Jung*, 422 F.3d 630 (8th Cir. 2005).

283. See e.g., *World of Warcraft End User License Agreement*, *supra* note 271 (“You agree that you will not, under any circumstances . . . use cheats, automation software (bots), hacks, mods or any other unauthorized third-party software designed to modify the World of Warcraft experience . . .”).

284. See *Second Life Privacy Policy*, *supra* note 236 (“You retain any and all intellectual property rights you already hold under applicable law in Content you upload, publish, and submit to or through the Servers, Websites, and other areas of the Service, subject to the rights, licenses, and other terms of

Imagine a researcher who attempts to record a crowd scene in Second Life. Under standard copyright law, the researcher would be required to secure a license to film every avatar, structure, texture, and even article of clothing that appears.²⁸⁵ In response to this impracticable standard, Second Life developers have built a property covenant system to permit recorders to contact the owner of virtual land for permission to film.²⁸⁶

b. Defenses to Copyright Infringement

Researchers may be caught by surprise by copyright law in virtual worlds. The types of information that researchers collect in the physical world generally cannot be copyrighted. For example, an oral conversation between researcher and subject is not fixed in a medium.²⁸⁷ Even data that is fixed, for example, answers to a written survey, are too factual to be copyrightable.²⁸⁸ But in virtual worlds, every element of the world is subject to copyright protection. Thus, the researcher must secure consent not only from the subject of the study, but a license from the copyright owner, or must rely on some other defense to a claim of copyright infringement. Common defenses include sovereign immunity (for researchers acting in an official capacity for public institutions),²⁸⁹ consent or license,²⁹⁰ and fair use.²⁹¹

this Agreement, including any underlying rights of other users or Linden Lab in Content that you may use or modify.”)

285. Note that this is rarely a problem in the real world because realspace is not yet subject to copyright.

286. See *Snapshot and Machinima Policy*, SECOND LIFE WIKI, http://wiki.secondlife.com/wiki/Linden_Lab_Official:Snapshot_and_machinima_policy, at 2(a)(1)–(2) (last visited June 6, 2012) [hereinafter *Second Life Snapshot and Machinima Policy*] (requiring owner consent for snapshots only when the land covenant explicitly prohibits snapshots, but requiring owner consent for machinima unless the land covenant explicitly allows machinima). Note that I have predicted precisely this outcome: that the costs of serial negotiations for rights in virtual worlds would cause game gods to move from a contract-based regime to a property-based regime. See, e.g., Joshua A.T. Fairfield, *Anti-Social Contracts: The Contractual Governance of Virtual Worlds*, 53 MCGILL L. J. 427, 475 (2008) (“The promise of online communities will only be fully realized if the law protects private property and personal dignity as a matter of first principles, rather than relying on contracts to create all of the legal relationships that communities might need.”).

287. See *Fritz v. Arthur D. Little, Inc.*, 944 F. Supp. 95, 100 (D. Mass. 1996) (“If true, th[e] claim that the source of the allegedly infringing materials was not ‘fixed in any tangible medium of expression’ when copied would defeat Fritz’s claim of copyright infringement. ‘Original’ words spoke aloud can be copied (and independently copyrighted) by all, if they have not previously been fixed in a tangible medium of expression.”) (quoting 17 U.S.C. § 102(a)).

288. See, e.g., *Edwin K. Williams & Co. v. Edwin K. Williams & Co.-East*, 542 F.2d 1053, 1060–61 (9th Cir. 1976) (employing a distinction between the mere *record* of information and the *conveyance* of information).

289. In 1990, Congress passed the Copyright Remedy Clarification Act, Pub. L. No. 101-553, 104 Stat. 2749 (1990) (codified at 17 U.S.C. §§ 501, 511 (2006)), which exposed states to copyright liability. However, several district courts have held that the law is an unconstitutional exercise of Congressional power. See, e.g., *Chavez v. Arte Publico Press*, 204 F.3d 601, 607 (5th Cir. 2000) (finding the CRCA “was not passed pursuant to a valid exercise of Fourteenth Amendment

Fair use is often the first defense that a layperson will mention, partly because the fair use statute explicitly includes research and partly because the defense has percolated far enough into common parlance that people may believe that it is a matter of common sense. But fair use is a legal concept with specific conditions for availability.²⁹² Courts have held researchers liable for copyright infringement despite the assertion of a fair use defense for research. For example, when Texaco researchers copied single articles out of trade journals for their own use, a court determined that fair use was not applicable.²⁹³ A fair use defense is much more likely to succeed when the alleged fair use is transformative.²⁹⁴ For researchers who copy directly from data sources, this important transformative factor can be difficult to establish.²⁹⁵ To safeguard their fair use defense, researchers should copy only data that is relevant to their research query. They should subsequently use the copyrighted information as raw material in the creation of a new set of information.²⁹⁶ Even when all of the necessary fair use precautions are taken, asserting a fair use defense is far from simple. Fair use

enforcement powers”); *Rodriguez v. Tex. Comm’n on the Arts*, 199 F.3d 279 (5th Cir. 2000) (same); *Mktg. Info. Masters, Inc. v. Bd. of Trs. of Cal. State Univ. Sys.*, 552 F. Supp. 2d 1088, 1094 (S.D. Cal. 2008) (same); *InfoMath, Inc. v. Univ. of Ark.*, 633 F. Supp. 2d 674, 679–80 (E.D. Ark. 2007) (same). This line of cases is particularly relevant to this Article because so many researchers are affiliated with universities, many of them public institutions. A researcher affiliated with a public institution may thus escape copyright liability by asserting sovereign immunity from the suit. *See, e.g., Mktg. Info. Masters, Inc.*, 552 F.2d at 1094 (allowing the defense).

290. *See* discussion *supra* Part III.B.2.a.

291. *See* 17 U.S.C. § 107 (2006) (permitting “fair use of a copyrighted work . . . for purposes such as criticism, comment, news reporting, teaching . . . scholarship, or research.”).

292. *See id.* (requiring an evaluation of “[t]he purpose and character of the use . . . [t]he nature of the copyrighted work . . . [t]he amount and substantiality of the portion used in relation to the copyrighted work as a whole; and . . . [t]he effect of the use upon the potential market for or value of the copyrighted work.”). The affiliation of a researcher with a commercial enterprise does not clearly exclude them from the fair use defense. *See Am. Geophysical Union v. Texaco, Inc.*, 60 F.3d 913, 921 (2d Cir. 1994) (cautioning against giving undue emphasis to commercial motivation when determining the availability of the fair use defense). Affiliation with a commercial enterprise comes into play more prominently in the analysis of the fourth factor, when the use at issue “supersedes” the use for which a consumer would usually purchase the original. *See Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579 (1994). The Supreme Court has adopted a sliding-scale approach that reduces the importance of commercial status when alleged fair uses are transformative. *See id.* (“[T]he more transformative the new work, the less will be the significance of other factors, like commercialism, that may weigh against a finding of fair use.”). This is because “the more transformative the new work, the less important the other factors, including commercialism, become.” *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 818 (9th Cir. 2003).

293. *See Am. Geophysical Union*, 60 F.3d at 931 (denying the fair use defense when researchers made copies of journal articles to keep in their offices).

294. *See Campbell*, 510 U.S. at 579 (“Although such transformative use is not absolutely necessary for a finding of fair use, the goal of copyright, to promote science and the arts, is generally furthered by the creation of transformative works. Such works thus lie at the heart of the fair use doctrine’s guarantee of breathing space within the confines of copyright . . .”).

295. *See Am. Geophysical Union*, 60 F.3d at 931 (holding that copying journal articles for purpose of keeping them on file for further research is not fair use).

296. *See Fitzgerald v. CBS Broad., Inc.*, 491 F. Supp. 2d 177 (D. Mass. 2007).

litigation is fact intensive and case by case. The issue is therefore costly to litigate and courts have not applied the doctrine in a predictable manner; this is especially true when the DMCA anticircumvention provisions are relevant to the case.²⁹⁷

The DMCA and basic contract law further encroach on the fair use doctrine to reduce its effectiveness.²⁹⁸ Courts have held that parties are free to give up fair use defenses by contract.²⁹⁹ In *Davidson & Associates v. Jung*,³⁰⁰ Blizzard Entertainment (via its then-parent company Davidson & Associates) sued the creators of BnetD, an alternative to Blizzard's Battle.net online service for real-time strategy games (RTS), including StarCraft, WarCraft, and Diablo.³⁰¹ The defendants argued, correctly, that they had a fair use defense for purposes of designing software that was interoperable with Blizzard's system.³⁰² However, the court ruled that the defendants had given up their fair use defense by clicking on the game's EULA, which required the user to give up the fair use interoperability defense.³⁰³ The court noted that private parties are "free to contractually forego [sic] the limited ability to reverse engineer a software product."³⁰⁴ Further, the court noted that parties can "contract away a fair use defense."³⁰⁵ For purposes of the current analysis, therefore, *Davidson & Associates* stands for the proposition that fair use defenses—including, presumably, those of researchers to engage in research despite copyrights in the chats they log or avatars they record—can be contracted away in an EULA.

The defense of consent—obtaining a license to use copyrighted materials for research purposes—can also be difficult for virtual worlds researchers to

297. Compare *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 346 (S.D.N.Y. 2000) (reasoning that the DMCA prohibits any circumvention not explicitly authorized by the copyright holder), with *Chamberlain Grp., Inc. v. Skylink Techs., Inc.*, 292 F. Supp. 2d 1040, 1046 (N.D. Ill. 2003) (reasoning that the fair use provisions of the Copyright Act implicitly authorized defendants to circumvent control measures for the purpose of making fair use of the material).

298. At least one commentator has predicted that, while unavailable now, a "fair circumvention" defense will develop to protect fair users from DMCA liability for the measures they take to access copyrighted material. See *Armstrong*, *supra* note 280, at 3 ("[N]o court has yet gone so far as to hold that circumventing a technological protection measure is permissible under the DMCA in order to make a fair use of the underlying copyrighted work."). For examples of such refusals, see, for example, *Reimerdes*, 111 F. Supp. 2d at 321–24 (analyzing the doctrine of fair use); *Universal Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001). See also *Armstrong*, *supra*, at 280 (arguing that decisions "permit[ing] defendants to circumvent traffic in circumvention devices . . . gain persuasive force . . . if contextualized within the long history of judge-made exceptions to the general provisions of federal copyright law" and that courts should openly embrace this developmental reasoning).

299. See *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005).

300. See *id.*

301. *Id.* at 633.

302. *Id.* at 639.

303. See *id.* (quoting *Bowers v. Baystate Techs, Inc.*, 320 F.3d 1317, 1337 (Fed. Cir. 2003)) ("[A] state can permit parties to contract away a fair use defense . . . if the contract is freely negotiated.").

304. *Id.*

305. *Id.*

successfully raise. Consent works if the subject of the research owns the text and images.³⁰⁶ Most game EULAs do not, however, permit players to retain ownership of the intellectual property that they generate as part of the game. Blizzard Entertainment's *World of Warcraft*,³⁰⁷ for example, does not recognize player ownership of in-game intellectual property.³⁰⁸ The player cannot give consent for copying of the player's avatar at the same time that the player undertakes to become a research subject. When obtaining consent for virtual worlds research, it is important to secure copyright consent from the game god³⁰⁹ and human subjects research consent from the research subject.

c. Implications of Copyright and Licensing Law for Virtual Worlds Research Tools

i. Add-Ons

The constraints imposed by game gods on the characteristics and uses of add-ons pose novel challenges for researchers, who may find that the EULA of the virtual world in which they are studying changes in the middle of an experiment, thus requiring changes to the research methodology.³¹⁰ There are two reasons to be particularly cautious about complying with the EULA terms

306. See *Davis v. Blige*, 505 F.3d 90, 98 (2d Cir. 2007) (citing *T.B. Harms v. Eliscu*, 339 F.2d 823, 825 (2d Cir. 1964)) ("Owners may license others to exercise these rights or assign the rights to others.").

307. *World of Warcraft* is the largest and most successful game-style virtual world to date. Blizzard—the creator of *World of Warcraft*—has proven particularly litigious against add-on developers and remarkably aggressive in banning accounts for EULA transgressions. Blizzard's EULA is also fairly typical of virtual world EULAs. For all of these reasons, Blizzard serves as a useful tool for analyzing the intersection of virtual world research and copyright issues.

308. See *World of Warcraft End User License Agreement*, *supra* note 271 ("All title, ownership rights and intellectual property rights in and to the Game and all copies thereof (including without limitation any titles, computer code, themes, objects, characters, character names, stories, dialog, catch phrases, locations, concepts, artwork, character inventories, structural or landscape designs, animations, sounds, musical compositions and recordings, audio-visual effects, storylines, character likenesses, methods of operation, moral rights, and any related documentation) are owned or licensed by Blizzard."); see also *World of Warcraft Terms of Use*, *supra* note 270 ("All rights and title in and to the Service (including without limitation any user accounts, titles, computer code, themes, objects, characters, character names, stories, dialogue, catch phrases, locations, concepts, artwork, animations, sounds, musical compositions, audio-visual effects, methods of operation, moral rights, any related documentation, 'applets' incorporated into the Game Client, transcripts of the chat rooms, character profile information, recordings of games played using the Game Client, and the Game Client and server software) are owned by Blizzard or its licensors.").

309. This assumes that the EULA forbids the kind of copying in which the researcher wishes to engage. Many do not and others even expressly permit machinima (recording) or snapshots under certain conditions.

310. See *World of Warcraft Terms of Use*, *supra* note 270 ("Blizzard may change, modify, suspend, or discontinue any aspect of the Game at any time."); see also *Second Life Terms of Service*, *supra* note 39 ("This Agreement may be changed by Linden Lab By continuing to access or use Second Life after the effective date of any such change, you agree to be bound by the modified Terms of Service.").

regarding add-ons in a virtual world. First, of course, the researcher will not wish to violate copyright law. Second, the researcher will also not wish for subjects to risk litigation.

Putting a human subject at risk of a lawsuit poses more than a minimal risk of harm to research subjects.³¹¹ A central concern is that the use of a given research add-on might be deemed “unauthorized” by a game god,³¹² thus subjecting study participants to potential sanctions and violating the ethical principal of beneficence, or the “no harm” principle. There are two potential harms. The first risk is the harm of a lawsuit for copyright infringement. This risk seems unlikely to materialize, since even the most litigious game gods have not sued customers even in clear-cut cases of infringement by unauthorized add-ons.³¹³ The second risk is that the game god would terminate the player’s account for running an unauthorized add-on. Game gods regularly ban accounts for the use of unauthorized add-ons.³¹⁴ Harm to an account constitutes true harm, in the sense that virtual objects, avatars, possessions, and real estate are “real”—and therefore really valuable—to the player.³¹⁵ Thus, a researcher should ensure that the researcher’s use of add-ons does not contravene the EULA—not for the researcher’s sake, but for the sake of the subjects.

Add-ons are permitted only on sufferance of the game god. Game gods permit users to design and implement add-ons both as a method for improving the game experience and as a means of crowdsourcing interface design.³¹⁶ The best add-ons are often incorporated into the game user interface by the game god.³¹⁷ However, add-ons also permit players to perform acts that they would

311. See Protection of Human Subjects, *supra* note 126, at 60635 (defining more than minimal risk as conduct placing subject “at risk of criminal or civil liability or being damaging to the subjects’ financial standing, employability, insurability, reputation, or being stigmatizing”).

312. See *World of Warcraft Terms of Use*, *supra* note 270 (disallowing the “use [of] any unauthorized third-party software that intercepts, ‘mines’ or otherwise collects information from or through the Game or the Service” and regarding “any use of the Service or the Game Client in violation of the License Limitations will be regarded as an infringement of Blizzard’s copyrights in and to the Game”).

313. See *MDY Indus., LLC v. Blizzard Entm’t, Inc.*, 629 F.3d 928 (9th Cir. 2010) (detailing the lawsuit of Blizzard Entertainment against MDY Industries, and not the thousands of users of the developer’s program).

314. See Jeremy Reimer, *Blizzard Bans 30,000 World of Warcraft Accounts*, ARS TECHNICA (June 12, 2006, 1:59 PM), <http://arstechnica.com/old/content/2006/06/7033.ars> (Blizzard banned 30,000 accounts for EULA violations in a single month).

315. See MCKEE & PORTER, *supra* note 33, at 119 (“[V]irtual does not mean ‘not real.’”).

316. See *id.* (“With the continuing popularity of World of Warcraft user interface add-ons created by the community of players, Blizzard Entertainment has formalized design and distribution guidelines . . . [that] help promote an enjoyable gaming environment for all of our players . . .”).

317. See, e.g., Tudor Stefanescu, *World of Warcraft Raiding Made Easy with CT Raid Assist*, SOFTPEDIA (Oct. 18, 2006), <http://news.softpedia.com/news/World-of-Warcraft-Raiding-Made-Easy-With-CT-Raid-Assist-38235.shtml>.

normally not be able to perform.³¹⁸ Conflicts over add-ons can grow into full-fledged litigation.

For example, *MDY Industries, LLC v. Blizzard Entertainment, Inc.*³¹⁹ arose after Blizzard claimed that MDY and its owner, Michael Donnelly, creators of the interface add-on WoWGliders (Glider), infringed Blizzard's copyright.³²⁰ Glider was automation, or "bot" software, that permitted the player to play the game without being physically present at the keyboard.³²¹ This practice was called "botting," since the automated avatar is functionally a robot.³²² Blizzard decided that the ability to bot a World of Warcraft avatar detracted from the overall enjoyment of the game for other players.³²³ Thus, it banned botting in the EULA. However, numerous players ignored the prohibition and used Glider to automate their avatars.³²⁴

The district court found first that the World of Warcraft players who used Glider were in violation of the EULA, and therefore were primary infringers of copyright since they were playing the game in contravention of the license.³²⁵ The district court then found the add-on developer secondarily liable for creating the add-on that permitted the primary infringement of the players.³²⁶

The Ninth Circuit reversed on the finding of primary infringement,³²⁷ but not on grounds that should prove particularly comforting to human subjects accused of violating game gods' EULAs. The Ninth Circuit found that the promise not to use unsanctioned automation software constituted a contractual covenant, not a license condition.³²⁸ Thus, users who used automation software were in breach of contract, not violating copyright based on the WoW EULA as

318. See *AddOn*, *supra* note 265 ("AddOns are generally self-contained User Interface (UI) modification components In plain English, an AddOn is just some files you can put in your game folder that can (theoretically) improve your interaction with the World of Warcraft game (i.e. make it easier to play, or give you more information about what's going on in the game).").

319. See *MDY Indus., LLC v. Blizzard Entm't, Inc. (MDY I)*, No. CV-06-2555-PHX-DGC, 2008 U.S. Dist. LEXIS 53988 (July 14, D. Ariz. 2008); see also *MDY Indus., LLC v. Blizzard Entm't, Inc. (MDY II)*, 616 F. Supp. 2d 958 (D. Ariz. 2009).

320. See *MDY I*, 2008 U.S. Dist. LEXIS 53988; see also *MDY II*, 616 F. Supp. 2d 958.

321. See *MDY II*, 616 F. Supp. 2d at 961–62.

322. See *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1060–61 (2000) ("A software robot is a computer program which operates across the Internet to perform searching, copying and retrieving functions on the websites of others. A software robot is capable of executing thousands of instructions per minute, far in excess of what a human can accomplish.").

323. See *MDY II*, 616 F. Supp. 2d at 963 ("[World of Warcraft] is a carefully balanced competitive environment where players compete against each other and the game to advance through the game's various levels and acquire game assets. Glider upsets this balance by enabling some payers to advance more quickly, diminishing the game experience for other players.").

324. See *id.* (noting that in five years "[WoWGliders] has sold more than 100,000 copies").

325. See *MDY I*, 2008 U.S. Dist. LEXIS 53988, at *10–12, *18–19 (finding that in using Glider, players had violated the EULA, and thus infringed Blizzard's copyright).

326. *Id.*

327. *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 941, 958 (9th Cir. 2011).

328. *Id.* at 939–41.

written.³²⁹ But the Ninth Circuit left the door open for a company to expressly make an anti-botting provision a condition of the license (which, in this Author's estimation, most virtual world licenses do). Further, whether a subject violates a license condition or a mere contractual promise does not bear on the penalty most users will actually face for using unsanctioned automation software: being banned from the virtual world for breach of the contract.³³⁰ If a researcher causes a subject to violate the EULA by means of installing an add-on, this could mean an account suspension for the subject, account termination, or at worst, litigation against both subject and researcher.

This does not mean that all research add-ons are prohibited. Indeed, some games have formal mechanisms for determining whether or not an add-on is permitted. The World of Warcraft EULA prohibits “any unauthorized third-party software that intercepts, ‘mines’, or otherwise collects information from or through the Game or the Service . . . provided, however, that Blizzard may, at its sole and absolute discretion, allow the use of certain third party user interfaces.”³³¹ Second, the EULA notes that “[y]ou agree that you will not, under any circumstances . . . in whole or in part, copy, photocopy, reproduce, translate, reverse engineer, derive source code from, modify, disassemble, decompile, or create derivative works based on the Game.”³³² Thus, it is clear that any unauthorized program that “collects information from or through”³³³ the service may operate only at the game god's sufferance—that is, whether the add-on is an unauthorized add-on.

The question of whether the add-ons are unauthorized or not depends on Blizzard's UI Add-On Development Policy.³³⁴ That policy requires that add-ons be “free of charge”; make their code “viewable by the general public”; “not negatively impact” players or gameplay; “not include advertisements”; “not solicit donations”; not contain offensive or objectionable material”; “abide by [the] World of Warcraft TOU and EULA”; and the game god retains the “right to

329. *Id.* at 941.

330. *Id.* at 938–39.

331. See G.N. Allen et al., *Ethical Approaches to Robotic Data Gathering in Academic Research*, 1 INT'L J. INTERNET RES. ETHICS 1, 10–11 (2008) (“However, at the same time that they open and facilitate new avenues of research, automated data collection agents present new ethical challenges, as the features of automated agents that make them most appealing for research use also raise issues as to their impact upon targeted web-sites.”); see also *id.* at 15–16 (“When academic researchers deploy automated data collection bots, they can collect very large amounts of data in relatively short periods of time, but this power comes at a cost—a cost only partly borne by the researcher. Both data collection bots and resource discovery bots . . . use the resources of web servers in ways that may not have been intended by the owners of those resources. Repeated interaction with the web site being accessed places some load on the equipment of the owners or hosting agent . . .”).

332. See *World of Warcraft End User License Agreement, Additional License Limitations*, BLIZZARD, http://us.blizzard.com/en-us/company/legal/wow_eula.html (last visited June 6, 2012).

333. *Id.*

334. See *UI Add-On Development Policy*, WORLD WARCRAFT, <http://us.battle.net/wow/en/forum/topic/1021053914> (last visited June 6, 2012).

disable any add-on functionality.”³³⁵ A research add-on that meets these criteria is unlikely to be deemed an unauthorized add-on, unlikely to cause the harm of account suspension, and thus unlikely to violate the requirements of human subjects research law.

ii. Recording, Machinima, and Framecapture

The other commonly studied virtual world is Second Life. For researchers, at least, Second Life looms large because it is the most well-known purely social virtual world. Second Life is also enticing to researchers because it embraces a real money economy. The Second Life EULA does not prohibit exchanging real-world currency for in-world items of value, which makes in-world economic and behavioral studies particularly common.³³⁶ An examination of the Second Life TOS is therefore useful to describe and predict the kinds of challenges researchers will face in so-called “social” virtual worlds.

The Second Life TOS contains several provisions that bear on the ability of researchers to use framecapture software to record a subject’s behavior within the world. On March 31, 2010, Linden Lab implemented significant changes to the Second Life TOS that impact when parties may record video or take snapshots in Second Life. It is worthwhile, therefore, to review the Second Life TOS changes, as they may potentially impact common research methodologies.³³⁷ The goal here is to examine how contractual change can have a serious impact on research methodology in a heavily researched virtual world.³³⁸

The changes required anyone seeking to film or record video within the virtual world (termed “machinima”³³⁹ in gamerspeak and in the TOS) or still screenshots (termed “snapshots”) to secure the consent of the owner of the land on which the recording is to take place. Additionally, the TOS required consent from any avatar that is identifiable in a video (but not in a snapshot).³⁴⁰ The

335. *Id.*

336. The very fact that economic and behavioral studies are more common in worlds that allow real money economies drives home the point that virtual world users care deeply about their virtual world communities. Studies are more common where observable behavior is more common. Observable behavior is more common when users are not concerned about the welfare of their virtual presence. Therefore, the fact that economic behavior in Second Life is not an offense punishable by suspension is exactly why researchers are able to more easily study that behavior. If researchers refuse to take seriously the adverse consequences of their study methods on the participants, their subject pool will evaporate because virtual world users will not be willing to take part in research behavior exposing them to account suspension.

337. Common programs for frame capture include Camtasia, *available at* <http://www.techsmith.com/camtasia.html>, and Fraps, *available at* <http://www.fraps.com>.

338. This examination is more important than the question of the Second Life contract itself, which—like many game EULAs—changes constantly.

339. *See Second Life Snapshot and Machinima Policy*, *supra* note 286 (Machinima is defined as “a film or computer animation generated using the real-time three-dimensional graphics-rendering engine of Second Life.”).

340. *See Second Life Terms of Service*, *supra* note 39.

Snapshot and Machinima Policy contains the relevant alterations to the Second Life agreement.³⁴¹ According to the policy, to “capture machinima means to film or record machinima.”³⁴² Thus, the filming or recording of subjects in Second Life using Camtasia or Fraps would constitute the creation of machinima. In Second Life, the users are the ones who could potentially be suspended for recording, not the researchers who direct them to do so.³⁴³

Section 7.4 of the revised Second Life TOS incorporates the Second Life Machinima and Snapshot Policy.³⁴⁴ That policy adds two requirements for recording machinima within Second Life.³⁴⁵ First, parties seeking to record machinima must abide by covenants governing the land on which the proposed recording would be made.³⁴⁶ More importantly, the covenant must expressly *allow* machinima in order for the machinima recording to comply with the TOS.³⁴⁷ If the covenant does not expressly allow machinima—even if the covenant does not mention machinima³⁴⁸—the party seeking to record machinima must contact the owner of the land and seek permission to film or record.³⁴⁹

Independent of the obligation to only record machinima on land that expressly permits it by covenant, parties seeking to record machinima must seek consent to record all avatars who are named in the machinima or who are sufficiently distinctive in appearance that they would be recognizable from the recording.³⁵⁰ Consent is not required if the avatar is not recognizable and is a member of a crowd scene or appears only fleetingly in the background.³⁵¹

The second change to the Second Life TOS focuses on snapshots. There are

341. See *Second Life Snapshot and Machinima Policy*, *supra* note 286 (requiring owner consent for snapshots only when the land covenant explicitly prohibits snapshots, but requiring owner consent for machinima unless the land covenant explicitly allows machinima).

342. *Id.*

343. See discussion *supra* Part III.B.c (explaining that contract governance of virtual worlds gives game developers the power to restrict or terminate a user’s account when researchers direct them to take actions that violate the agreement).

344. *Id.*

345. *Id.*

346. See *id.* at Part III.B.2.c.ii (requiring party desiring to record machinima to “check whether the covenant for the land *allows* machinima”). Because Second Life allows users to buy, own, and manage virtual real estate, it allows owners to set terms of use or covenants to govern behavior of avatars who enter that land.

347. See *id.*

348. See *id.* at Part III.B.2.c.ii (If the covenant does not allow machinima or doesn’t address machinima, then you need special permission from the landowner to capture machinima.).

349. *Id.*

350. See *id.* at Part III.B.2.c.ii (For machinima, you must have the consent of all Residents whose avatars or Second Life names are featured or recognizable in the machinima. This includes avatars who are featured in a shot, avatars whose names are legible, and avatars whose appearance is sufficiently distinctive that they are recognizable by members of the Second Life community. Consent is not required if an avatar is not recognizable and is merely part of a crowd scene or shown in a fleeting background. Consent is not required for any snapshots.).

351. See *id.*

fewer restrictions on snapshots than machinima. Avatar consent is not required for snapshots; however, parties taking snapshots must comply with the covenants governing land.³⁵² If the covenant prohibits snapshots, then the party seeking to take a snapshot must obtain consent from the landowner first.³⁵³ However, if the land covenant does not expressly mention snapshots, parties are free to take them.³⁵⁴ The best practice for complying with the updated Second Life TOS is to limit filming or recording to land owned by the research team. This permits recording without concern for land covenants and enables researchers to obtain the consent of each avatar that they intend to record as part of the recruitment process. In addition, some research teams may opt to use a “travelogue” methodology, in which the subject reports on the subject’s own gameplay experience while taking snapshots—not machinima—to supplement the narrative. Similarly, participant observers often supplement their detailed observational narrative with screenshots. To the extent that these methodologies are employed in Second Life, subjects or participant observers should be instructed to comply with the snapshot policy in compiling the travelogues.

Of course, any further significant change in policy could immediately undermine the usefulness of the best practices outlined here. These sudden changes elucidate the challenges of conducting research in a shifting legal climate. Whenever the game developers alter their EULAs—and wherever possible, game developers will undoubtedly make alterations that limit their own liability as the law develops—acceptable research standards may change. Researchers must be constantly aware of the contractual provisions governing the relevant virtual world and take pains to ensure that they and their subjects comply.

iii. Robotic Data Gathering, Spiders, and Scrapers

A related but distinct source of concern is robotic data gathering, or “scraping”³⁵⁵ of a virtual world’s application programming interface. Research ethicists have noted that the ethics of scraper use depend largely on the degree to which the scraper increases server load.³⁵⁶ From the legal perspective, website scraping (for example, a competitor auction site’s scraping of eBay’s auctions) is

352. *See id.* (For snapshots, check whether the covenant for the land prohibits snapshots. If it does, then you need special permission from the landowner to take the snapshot. If it allows snapshots or doesn’t address them, then you do not need special permission from the landowner as long as you comply with any terms that may be in the covenant).

353. *Id.*

354. *Id.*

355. “Scraping” is the use of a computer program written to automatically collect data from the Internet generally, or specifically from a particular website or virtual world. These programs are often referred to as bots, scrapers, or spiders. *See Web Scraping Software*, MOZENDA, <http://www.mozenda.com/web-scraping-software> (last accessed Feb. 18, 2012).

356. *See* G.N. Allen et al., *supra* note 331, at 10–11.

akin to trespass.³⁵⁷ Courts have adopted cybertrespass as grounds for preventing unauthorized scraping of electronic databases, on the theory that the scraping bot is “trespassing” on the property of the scraped party.³⁵⁸ The use of trespass theories to limit scraping software is problematic for researchers. Although there may be a fair use right to make use of intellectual property—however attenuated by judicial interpretation—there is no similar right to trespass on property for purposes of research. Scraping software therefore poses risks independent of the risk of being deemed an unauthorized add-on, as it may run into difficulties on websites that wish to prevent automated access to databases.

There is some risk in proceeding with the use of scraping software without the consent of the scraped party. However, if the researcher is solely responsible for running the scraper, then the researcher alone runs the risk of litigation under cybertrespass theories. This is unlike intellectual property infringement theories, where an add-on run locally on a subject’s machine could cause a court to find the research subject liable for copyright infringement.³⁵⁹ While the litigation risk to a researcher who does not secure consent from a game god to scrape a virtual world or database is not trivial, the risk to the subjects of the experiment from scrapers seems negligible. A research subject in a virtual world necessarily has agreed to the EULA and has been granted permission to move within the world; therefore, the subject is incapable of “trespass.” Prudent researchers should be concerned about the implications of data scraping, but this Article is more focused on the violations of the Common Rule that result from failing to minimize the harm to human subjects—harms that proceed on intellectual property theories rather than trespass theories.

3. *Privacy Law*

Researchers and IRBs must also consider privacy law—both common law and statutory—in experimental design. This section will examine the common law privacy torts and will provide an analysis of when federal and state privacy statutes may impact researchers in virtual worlds.

a. Privacy Torts

Common law causes of action are often the first to be applied to novel technological problems.³⁶⁰ For example, the law of trespass quickly came to

357. See, e.g., *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp 2d. 1058 (N.D. Cal. 2000) (holding that auction rival Bidder’s Edge’s use of scraping technology constituted trespass on the computer systems of eBay).

358. See G.N. Allen et al., *supra* note 331, at 18–20 (discussing cases in which courts have found parties who use scraping bots liable for trespass).

359. See discussion *supra* Part III.B.2.c.

360. See G.N. Allen et al., *supra* note 331, at 18–20.

govern bots, scrapers, spammers, and aggregator sites.³⁶¹ Defamation has applied seamlessly to blogs.³⁶² The medieval principles of trespass to chattels were used to determine whether a company could sue for unwelcome e-mails sent to company employees.³⁶³

Likewise, the development of privacy torts in the United States has followed this pattern. Justices Warren and Brandeis's foundational article, *The Right to Privacy*,³⁶⁴ was a response to technology—the camera. Warren and Brandeis wrote:

Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.” For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer.³⁶⁵

Warren and Brandeis presciently described law's evolution in response to technological change as well as the threat that technological advances pose to human dignity by undermining privacy interests. Warren and Brandeis's core insight was that “the existing law affords a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds.”³⁶⁶ This insight applies a fortiori to virtual worlds, which are by nature enormous cameras.³⁶⁷

Virtual worlds are on the forefront of emerging technologies, so it makes sense that the common law will develop in response to them. The topics of this Article are therefore relevant to legal scholars and game developers as well as human subjects researchers.

The most common privacy tort brought against researchers is termed public disclosure of private facts, known in some states as “invasion of privacy.”³⁶⁸ This

361. *Id.*

362. *See, e.g., In re Perry*, 423 B.R. 215, 269–70 (Bankr. S.D. Tex. 2010) (observing that defamatory statements are “published” when they are written in a blog or even when a link to the blog is sent in an e-mail); *Doe v. Cahill*, 884 A.2d 451, 457 (Del. 2005) (discussing the requisite standard for a defamation plaintiff to obtain the identity of anonymous blog author).

363. *See, e.g., Intel Corp. v. Hamidi*, 71 P.3d 296, 304 (Cal. 2003) (noting that “decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers' functioning”).

364. Samuel D. Warren & Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193, 195 (1890).

365. *Id.*

366. *Id.* at 206.

367. *See* discussion *infra* Part III.B.2.c (describing methods of recording in virtual worlds).

368. *See Hargrave v. G.E. Aviation Sys. L.L.C.*, No. 8:08-cv-1966-T-30MAP, 2009 WL 2340654 (M.D. Fla. 2009) (denying recovery for invasion of privacy against lab researchers).

tort requires publication of private facts that are not newsworthy and the publication of which is highly offensive to a reasonable person.³⁶⁹ Publication among research colleagues may not be sufficient to support the cause of action,³⁷⁰ but publication of private facts in a publicly accessible research study is certainly sufficient to satisfy the publication element.³⁷¹ Facts that are completely disassociated from the human subject's identity may not be sufficiently private to support this cause of action, so researchers should remove identifying bits of information wherever possible.³⁷²

What constitutes "identification" can also be tricky. While some avatars are pseudonyms, researchers should not assume that they are safe to publish.³⁷³ One court has suggested that a researcher's use of initials to refer to an unnamed human subject is appropriate because initials are not sufficiently identifiable.³⁷⁴ However if an identifier were sufficiently identifiable to the subjects' real-world identity, publication of information about the subject could be grounds for an invasion of privacy tort.³⁷⁵ This is troubling for virtual worlds researchers because subjects are often well known by their avatar names.³⁷⁶ Personally chosen avatar names and carefully constructed avatar images are much more personally identifiable than the minimally identifiable information presented by two letters—two letters out of twenty-six, which could stand for hundreds of thousands of name combinations. The purpose of an avatar is to be personally identifiable. Researchers should therefore redact avatar identities from their publications.

If identification is absolutely required to establish the legitimacy of the study,

369. See *Taus v. Loftus*, 151 P.3d 1185, 1207 (Cal. 2007) (outlining the elements of the tort).

370. See, e.g., *Hargrave*, 2009 WL 2340654 (holding that providing an employee blood sample to three lab workers for analysis did not constitute sufficient publication to support invasion of privacy tort in Florida, which adopts the Restatement's formulation of the tort).

371. See, e.g., *Vargas v. Shepherd*, 903 N.E.2d 1026, 1031 (Ind. Ct. App. 2009) ("[T]he publicity element requires communication to the public at large or to so many persons that the matter is substantially certain to become one of public knowledge . . . [A] few courts have adopted a looser definition . . . allow[ing] a disclosure to be actionable . . . as long as it is made to a 'particular public' with a special relationship to the plaintiff."); see also *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633, 648–49 (Cal. 1994) ("[C]ommon law invasion of privacy by public disclosure of private facts requires that the actionable disclosure be widely published and not confined to a few persons or limited circumstances.").

372. See *Adams v. King Cnty.*, 192 P.3d 891, 902 (Wash. 2008) ("While a research facility may eventually have assimilated its research of Jesse's brain into data as part of a scientific publication, such filtered information likely would no longer contain any recognizable private matters connected to Jesse . . . [T]he trial court properly dismissed Adams's privacy claim.").

373. See discussion *infra* Part II (discussing the deliberate creation of avatars as personal representations).

374. See *Taus*, 151 P.3d at 1211 (doubting that mere initials could be used to identify the plaintiff in a privacy tort action).

375. See *id.* (rejecting privacy tort action because information released by researchers was not sufficiently identifiable, not because information released was somehow privileged by its research context).

376. See *Penney*, *supra* note 5, at 221 ("The avatar is a 3D character that is completely controlled by the member the avatar is the person in the virtual world.").

researchers may be able to rely on the newsworthiness factor to insulate themselves from liability.³⁷⁷ Researchers should be especially careful to avoid publishing facts that the user could reasonably expect to be private.³⁷⁸ Courts have interpreted “newsworthiness” to include interest in a specific field of research.³⁷⁹ This is an important protection for researchers who publish private facts. So long as the discoveries gleaned from the research are of interest to researchers in the field, the plaintiff will not succeed in a privacy action.³⁸⁰

Researchers have also been subject to suit for a second privacy tort: intrusion on seclusion, also known as intrusion into private matters.³⁸¹ This tort requires an intentional intrusion into a private place, conversation, or matter in a manner highly offensive to a reasonable person.³⁸² This tort is more dangerous for researchers because free speech protections are not present.³⁸³ Liability attaches at

377. See *Haynes v. Alfred A. Knopf, Inc.*, 8 F.3d 1222, 1233 (7th Cir. 1993) (citing *Gilbert v. Medical Econ. Co.*, 665 F.2d 305, 308 (10th Cir. 1981)) (“Reporting the true facts about real people is necessary to ‘obviate any impression that the problems raised in the [book] are remote or hypothetical.’”); see also *Taus*, 151 P.3d at 1208 (“[T]he facts disclosed—relating generally to how the experiences described in the case study may have affected Jane Doe’s subsequent conduct and career as an adult—clearly are newsworthy, and for that reason cannot properly be the basis of such a tort action.”).

378. What constitutes a reasonable expectation of privacy in virtual worlds is especially difficult to pin down. Some courts have suggested that posting facts in social media renders them public and eliminates the public disclosure of private facts action for that plaintiff. See *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 1130 (2009) (holding that the posting of a poem on a personal MySpace.com page rendered the contents of the poem public despite the poster’s expectation of a “limited audience”). Even in this case, however, the court acknowledged that “[i]nformation disclosed to a few people may remain private.” See *id.* (citing *M.G. v. Time Warner, Inc.*, 89 Cal. App. 4th 623, 632 (2001)). Actions taken and words spoken in virtual worlds with the expectation that only a few fellow users be privy to them might still be considered private despite their online presence.

379. See *Taus*, 151 P.3d at 1208 (“In light of the prominence of the Jane Doe case study in the repressed memory field, we find that the disclosure of such facts was newsworthy.”).

380. See *id.* at 1208–09 (dismissing the public disclosure of private facts action because the facts were newsworthy).

381. See *id.* at 1212–13 (allowing an intrusion on seclusion action against researchers).

382. See *id.* at 1212 (describing the elements of the tort of intrusion into private matters).

383. See *id.* at 1205–12 (dismissing the public disclosure of private facts action because of the newsworthiness of the facts while accepting the intrusion on seclusion action because newsworthiness did not enter into the analysis for that tort); see also *Schulman v. Group W Prods., Inc.*, 955 P.2d 469, 493 (Cal. 1998) (acknowledging that “the First Amendment does not immunize the press from liability for torts or crimes committed in an effort to gather news . . .”). But note that the legitimacy of the information seeking might go to the second element—the offensiveness—of the intrusion. See *id.* (“In deciding, therefore, whether a reporter’s alleged intrusion into private matters (i.e., physical space, conversation or data) is ‘offensive’ and hence actionable as an invasion of privacy, courts must consider the extent to which the intrusion was, under the circumstances, justified by the legitimate motive of gathering the news.”). *Schulman* relates to news gatherers getting a single, unique story which probably cannot be gathered at any other time or place from any other person, and so newsgathering weighs on the court’s analysis. In the research context, the information sought is one tiny piece of a large set of data that can ostensibly be gathered from any number of participants; therefore, the newsgathering issue probably will not be as important to intrusion on seclusion claims

the time of intrusion, not publication. The “private matter” element of this tort depends on the plaintiff’s objectively reasonable expectation of privacy.³⁸⁴ These expectations can be extremely counterintuitive and vary widely depending on the culture specific to the virtual world the researcher is studying.³⁸⁵ Thus, researchers must be cognizant of the norms present in virtual worlds.

Where a conversation happens may matter more than *how* the message is sent. Researchers must respect privacy of virtual places just as they respect privacy of physical places. “In MMOGs and virtual worlds, just as in real-world settings, individuals . . . interact in different, contextually based ways, some more personal and private, others more distant and public.”³⁸⁶ The ability of a qualitative virtual worlds researcher to ethically gather data will often depend on the pseudophysical context of the research.³⁸⁷ Researchers must be aware of the virtual world cultural norms that govern the world they are studying and adjust their data gathering accordingly.³⁸⁸ For example, the act of entering a house has different connotations in Second Life and World of Warcraft. In Second Life, the house belongs to someone who may have an expectation of privacy while within it.³⁸⁹ Thus, while it is possible to intrude even into a locked home in Second Life by rotating one’s virtual camera through a wall,³⁹⁰ doing so is a gross invasion of privacy. Similarly,

in the research context. *See Taus*, 151 P.3d at 1212 (ignoring the newsworthiness of collected data and upholding the plaintiff’s intrusion on seclusion cause of action).

384. *See Taus*, 151 P.3d at 1212 (“The tort is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation, or data source.”).

385. *See* discussion *infra* Part II. The context-specific expectation of privacy is not specific to virtual worlds; the whole reasonable expectation of privacy concept is a fact-specific inquiry. *See Taus*, 151 P.3d at 1227 (citing *Sanders v. Am. Broad. Co.* 978 P.2d 67, 72 (Cal. 1999) (“[P]rivacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law.”)).

386. MCKEE & PORTER, *supra* note 33, at 130.

387. *See, e.g., How Do I Get Some Privacy in Second Life?*, SECOND LIFE WIKI, http://wiki.secondlife.com/wiki/How_do_I_get_some_privacy_in_Second_Life%3F (last visited June 6, 2012) (describing various methods of insulating oneself from uninvited interruptions in Second Life).

388. *See* Heidi A. McKee & James E. Porter, *Playing a Good Game: Ethical Issues in Researching MMOGs and Virtual Worlds*, 2 INT’L J. INTERNET RES. ETHICS 5, 27 (2009) (citing a virtual world researcher: “One of the first dilemmas I had to address is the fact that *City of Heroes* has a ‘broadcast’ function in chat. This allows anyone on the server to input chat text so that it is sent to everyone on the server. There is also ‘local’ chat text which appears any time a toon is close to the toon chatting.”).

389. *See Community Standards*, SECOND LIFE, <http://secondlife.com/corporate/cs.php> (last visited June 6, 2012) (allowing all users a “reasonable level of privacy” and forbidding disclosing “personal information about your fellow Residents” or “disturbing the peace” through repetitive advertising or “following”).

390. *See* Cheyenne Palisades, *Breaking and Entering in Second Life*, CHEY’S SECOND LIFE BLOG (Dec. 27, 2006, 9:19 PM), <http://cheyennepal.blogspot.com/2006/12/breaking-and-entering-in-second-life.html> (“You probably already know that if you disable camera constraints and play with Camera Control, there’s not much you can’t do. You can, for instance, click on the wall of a dwelling, zoom in, and, by rotating the view, look about inside If you rotate your view inside a structure—even one with a locked door—and select an object and sit on it, you will instantly materialize on the

because virtual home walls are not physical, conversations can be heard through them.³⁹¹ Even so-called “public” chat³⁹² may actually be private when uttered in a user’s virtual home although it can be heard in the street outside. In World of Warcraft, a home may not have a particular connotation of privacy because players do not own homes. The players may, however, indicate an expectation of privacy by traveling to an out-of-the-way location. There are many intermediate points between the familiar “public” and “private” categorizations for communications.³⁹³ Many communications in virtual worlds are quasi-private: that is, restricted to a guild, party, or even group of friends.³⁹⁴ In the physical world, a speaker may limit conversations to a given geographic area by moderating the volume level or to a given audience by dialing certain phone numbers. Conversations in virtual worlds can be limited in the same way, whether to a “local” area around the user’s avatar or to a set of conversation partners specified by the users.³⁹⁵ Researchers must respect the changing expectations of privacy that go along with these changing conversation methods.

b. Statutory Privacy Regimes

This Section examines statutory regimes that bear on privacy in virtual worlds. Although statutes tend to adapt less quickly than does the common law, existing statutory regimes could be extended to apply to research activity in virtual worlds. After all, virtual worlds are to some extent three-dimensional renderings of the Internet; there is no reason why extant statutes dealing with conduct on the two-dimensional Internet should not be applied to the third dimension of online activity in virtual worlds. This Subpart addresses federal and international privacy laws that will likely bear on research activity in virtual worlds and then turns to state law privacy regimes.

object, inside the structure. Stand up, and you are free to explore. You have now broken and entered.”).

391. Tateru Nino, *Adjusting to a New World—Communicating by Chat*, SECOND LIFE INSIDER (Dec. 24, 2006, 10:30 PM), <http://podcasts.secondlifeinsider.com/2006/12/24/adjusting-to-a-new-world-communicating-by-chat> (describing the chat function, including the in-world chat ranges without regard to virtual walls).

392. That is, chat uttered in the /say channel.

393. See Frankel & Siang, *supra* note 33, at 8 (“[T]he same private vs. public distinction cannot be drawn for all computer mediated interactions, given the differences among the various types of [interactions] and the wide variations of groups that exist under each type.”).

394. See *id.* at 12 (“In the middle are MUDS (Multi-User Dungeons), where the address is available to the public, but participants are constrained by internally prescribed or available activities that are not considered public.”).

395. See, e.g., *Chat Channel*, SECOND LIFE WIKI, http://wiki.secondlife.com/wiki/Chat_channel (last visited June 6, 2012) (describing the functions of various public and private chat channels in Second Life).

i. Federal and International

The Children's Online Privacy Protection Act (COPPA)³⁹⁶ applies to "commercial websites and online services aimed at children"³⁹⁷ as well as general audience websites when the operator has actual knowledge that children's information is being gathered through the site.³⁹⁸ Such sites and services are required to seek parental consent before collecting or using personal information from a child under the age of thirteen.³⁹⁹ Under the act, website operators must post a notice that describes what information is collected from children, how it is used, how it is disclosed, must obtain verifiable parental consent, must inform parents upon request about information collected from a child, must give parents the right to revoke consent and have the information deleted, must provide a reasonable means for parents to review information collected from their children, must not condition participation in games on provision of information not necessary to participate in the activities, and must take steps to keep children's data secure.⁴⁰⁰

COPPA could therefore govern research collected via a commercial website.⁴⁰¹ Although COPPA is reserved for commercial websites or services, it would be triggered if a researcher were to knowingly collect and use personally identifiable information from children under thirteen through a commercial website (for example, via web surveys posted to a site). If a researcher who operates a commercial website obtains actual knowledge that data from children under thirteen is being gathered through that site, then the information must be deleted or the researcher must comply with COPPA.

Actual knowledge of this sort is a real possibility for researchers, since researchers may seek to parse certain types of behavior by age group. Thus, researchers may well come into possession of personally identifiable information about children, which is defined by the statute to be a real first and last name, address, telephone number, social security number, or "any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or . . . information concerning the child or the parents of that child that the website collects online from the child and combines with [any other identifier described in the section]."⁴⁰² For example, an avatar name coupled with a Facebook profile (which constitutes both a real name and a means of contacting the person via online means) would render the avatar information and everything about that avatar "personally identifiable information" due to the pairing with real-

396. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505 (2006).

397. See PROSKAUER ON PRIVACY § 4:1.3[A] (Kristen J. Matthews ed., 2011).

398. See 15 U.S.C. §§ 6501–6502 (2006).

399. *Id.*

400. *Id.*

401. *See id.*

402. *See id.* § 6501(8)(F)–(G).

world data.⁴⁰³ Indeed, it is entirely possible that an avatar name itself would be personally identifiable information, since it, like an e-mail address, can be used to contact the child.⁴⁰⁴

Researchers and IRBs may also find it useful to familiarize themselves with European data privacy law, since international research groups often work with both U.S. and European components. The European Union Data Privacy Directive imposes tight restrictions on the collection, processing, and export of personal data to countries outside of the European Union.⁴⁰⁵ If a researcher proposes to process and store data in the United States, the researcher must take care not to run afoul of the European Union's prohibition on moving data outside of the European Union to countries that offer lesser privacy protections.⁴⁰⁶ There are several solutions to the export problem: first, there is no prohibition on the export of anonymized data from the European Union,⁴⁰⁷ second, data may be exported with the subject's unambiguous consent,⁴⁰⁸ and third, U.S. companies may seek "safe harbor" status by accepting restrictions requiring them to treat data as if it is still physically in Europe and subject to the Directive.⁴⁰⁹ Doing so may prove restrictive, however, because data processing under the Directive is constrained. Among other limits, data may be only processed for the specific purpose for which it was collected, and collection, processing and retention may not be excessive in relation to that purpose.⁴¹⁰

Another commonly referenced privacy law is the Wiretap Act, which is the concatenation of Title I of the Electronic Communications Privacy Act and Title III of the Omnibus Crime Control and Safe Streets Act. The Wiretap Act prohibits "any person" from engaging in "the intentional interception of any wire, oral or electronic communication."⁴¹¹ Courts have determined that programs that run in the background and monitor a user's activity can constitute a violation of the Wiretap Act or similar state statutes.⁴¹² For example, a spouse who loaded a spyware program that took periodic screenshots of the user's screen and put them

403. Facebook's new personalized web initiative, the Open Graph protocol, makes the connection between commercial websites and personally identifiable information even more likely. See Caroline McCarthy, *Facebook F8: One Graph to Rule Them All*, CNET (April 21, 2010, 10:25 AM), http://news.cnet.com/8301-13577_3-20003053-36.html (describing the Open Graph protocol introduced at the April 2010 F8 Facebook Conference).

404. See *Instant Messages*, *supra* note 19 (discussing the use of avatar identities in Second Life to directly contact offline identities).

405. See PROSKAUER ON PRIVACY, *supra* note 397, § 14.2 (citing EU Directive 95/46/EC, 1995 O.J. (L 281) 31).

406. See EU Directive 95/46/EC, 1995 O.J. (L 281) 31, at ch. IV, art. 25 (EU) [hereinafter Directive].

407. See PROSKAUER ON PRIVACY, *supra* note 397, § 14:3.1.

408. See Directive, *supra* note 406, at ch. IV, art. 26.

409. See PROSKAUER ON PRIVACY, *supra* note 397, § 14:3.2.

410. See *id.* § 14:2.4[A] (citing Directive, *supra* note 406, at ch. 2, art. 6 (EU)).

411. See PROSKAUER ON PRIVACY, *supra* note 397, § 6:2.2 (citing 18 U.S.C. § 2511(1)(a)).

412. See *O'Brien v. O'Brien*, 899 So. 2d 1133 (Fla. Dist. Ct. App. 2005).

onto her husband's computer was held to have violated the Florida Security of Communications Act, a state law analog of the Wiretap Act.⁴¹³ However, “[u]nder section 2511(2)(d) [of the Wiretap Act], a party to a communication may record and disclose it as long as doing so is not “for the purpose of committing any criminal or tortious act.”⁴¹⁴ “Furthermore, a party can consent not only to his or her own interception, but interception by others as well.”⁴¹⁵ Thus, it appears that although the logging of communications from a nonparticipant in a study to a participant by a researcher does create autonomy concerns under *The Belmont Report* and the regulations implementing *The Belmont Report* found at 32 C.F.R. 219, logging with one party's consent does not constitute a violation of the Wiretap Act.

Title II of the Electronic Communications Privacy Act, commonly called the Stored Communications Act (SCA), is also relevant to virtual words research.⁴¹⁶ Whereas the Wiretap Act protects communications as they occur, the SCA protects communications in storage and provides for criminal liability for persons who access stored communications illegitimately⁴¹⁷ and for companies that release stored communications illegitimately.⁴¹⁸ The SCA generally does not apply to researchers who propose to work from data stored by the game gods. The SCA permits companies to disclose the contents of stored communications, and third parties to access such stored communications, as long as they have secured the consent of the account subscriber, the originator of the message, or the intended recipient of the message, to do so.⁴¹⁹

413. See PROSKAUER ON PRIVACY, *supra* note 397, § 6:2.2.

414. *Id.* § 6:2.4[B].

415. *Id.* (citing *Lewellen v. Raff*, 843 F.2d 1103, 1115 (8th Cir. 1988)).

416. See PROSKAUER ON PRIVACY, *supra* note 397, § 6:1.

417. See 18 U.S.C. § 2701(a) (2006) (“Except as provided in subsection (c) of this section whoever—(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.”).

418. See *id.* §§ 2701–2712; *id.* § 2702(a)(2) (“[A] person or entity providing a remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing . . .”).

419. See *id.* § 2702(b)(3) (noting that “[a] provider . . . may divulge the contents of a communication—(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service . . .”); see also *id.* § 2701(c) (“Subsection (a) of this section does not apply with respect to conduct authorized—(1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user . . .”).

Thus, for example, the EverQuest II User Agreement and Software License permits Sony Online Entertainment to monitor and record player interactions and communications and transmit that information in its sole discretion to third-party licensees.⁴²⁰ Other popular virtual worlds have similar, although not identical, EULA provisions.⁴²¹

The Federal Trade Commission (FTC) commonly enforces companies' stated privacy policies under its broad power to prevent unfair and deceptive trade practices under § 5 of the Federal Trade Commission Act. The Act provides that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."⁴²² Thus, if companies transmit information to third parties in contravention of their stated privacy policies, the FTC may determine that consumers have been injured and that the unauthorized disclosure constitutes an unfair or deceptive trade practice.⁴²³ There are several reasons to believe that such privacy enforcement by the FTC is unlikely. First, the FTC's ambit only extends to unfair or deceptive acts in or affecting commerce (although federal courts have expansively interpreted the set of private, noncommercial activities that can "impact" commerce).⁴²⁴ More importantly, as noted above, game god EULAs

420. See *Everquest II User Agreement and Software License*, SONY, [https://help.station.sony.com/app/answers/detail/a_id/12248/kw/EverQuest II User Agreement and Software License](https://help.station.sony.com/app/answers/detail/a_id/12248/kw/EverQuest+II+User+Agreement+and+Software+License) (last visited June 6, 2012) ("You acknowledge that any and all character data is stored and is resident on our servers, and any and all communications that you make within the Game (including, but not limited to, messages solely directed at another player or group of players) traverse through our servers, may or may not be monitored by us or our agents, *you have no expectation of privacy in any such communications and expressly consent to such monitoring of communications you send and receive. You acknowledge and agree that we may transfer Game and your Account information (including your personally identifiable information and personal data) to the United States or other countries or may share such information with our licensees and agents in connection with the Game.*").

421. See, e.g., *World of Warcraft Terms of Use*, *supra* note 270 ("Blizzard may monitor, record, review, modify and/or disclose your chat sessions, whether voice or text, without notice to you, and you hereby consent to such monitoring, recording, review, modification, and/or disclosure."); *Terms of Service Archive Through 29 April 2010*, SECOND LIFE, http://wiki.secondlife.com/wiki/Linden_Lab_Official:Terms_of_Service_Archive/Through_29_April_2010 (last visited June 6, 2012) (TOS slightly more restrictive of Linden Lab's ability to transmit personal information to third parties: "You acknowledge and agree that Linden Lab, in its sole discretion, may track, record, observe or follow any and all of your interactions within the Service. Linden Lab may share general, demographic, or aggregated information with third parties about our user base and Service usage, but that information will not include or be linked to any personal information without your consent.").

422. See 15 U.S.C. § 45(a)(1) (2006).

423. See PROSKAUER ON PRIVACY, *supra* note 397 § 4:3.3.

424. See, e.g., *Wickard v. Filburn*, 317 U.S. 111 (1942) (interpreting a farmer's consumption of wheat grown on his own land and never sold to have impact on commerce because it displaced purchases on the open market); see also *Gonzales v. Raich*, 545 U.S. 1 (2005) (holding that federal government had authority to regulate homegrown marijuana that was never offered for sale because it affected commerce on a similar displacement theory).

generally permit the transmission of data to authorized third parties; thus, such a transfer is not an unfair or deceptive practice.⁴²⁵

ii. State Law

State privacy laws could potentially impact researchers' obligations as they operate in the United States. California is particularly pertinent, both because California law generally extends to protect its citizens beyond its borders, and because numerous research concerns operate within California or intend to gather information from residents of California.⁴²⁶ Additionally, California has particularly robust pro-privacy case law.

California has enshrined the right to privacy in its state constitution.⁴²⁷ Because there is no state action doctrine for this provision of the California Constitution, public and private researchers alike could be held liable for violations of the privacy clause.⁴²⁸ California courts have held the privacy provision is directed at four types of conduct, two of which are relevant to research interests: the overbroad collection and retention of unnecessary personal information by government or business interests, and the improper use of information properly obtained for a specific purpose.⁴²⁹ Researchers must be sure to collect only information that is relevant to their inquiry and to properly dispose of personal information at the conclusion of their study. Researchers who engage in after-the-fact analysis of game-god-gathered data sets in the quantitative methodology are especially vulnerable to the improper use prohibition of the California privacy clause. Because these data sets are collected pursuant to a limited EULA and not to the carefully crafted informed consent required for human subjects research, researchers could be liable for using data—properly collected for the game gods' commercial purposes—for a different and improper research purpose.

425. See, e.g., *Everquest II User Agreement and Software License*, *supra* note 420.

426. See e.g., *Company Profile*, BLIZZARD, <http://us.blizzard.com/en-us/company/about/profile.html> (“Headquartered in Irvine, Calif., Blizzard Entertainment”) (last accessed Nov. 22, 2011); *Contact Linden Lab*, LINDEN LAB, <http://lindenlab.com/contact> (detailing headquarter location in San Francisco) (last accessed Nov. 22, 2011).

427. See CAL. CONST. art. 1, § 1 (“All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.”). The privacy provision is strict, but there is an allowance for incursions on privacy that are “justified by a compelling interest.” See *White v. Davis*, 533 P.2d 222, 234 (Cal. 1975). Because the law is self-executing, see *id.* at 234, it comprises its own cause of action and must be considered when drafting research methodologies for study in California. *Id.* at 234-35.

428. See *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633 (Cal. 1994) (holding that the privacy provision of the California Constitution can be interpreted with reference to the ballot pamphlet that approved it, and that the presence of both government and business entities as targets of the provision show that the enactment is enforceable against nongovernmental entities in California).

429. See *White v. Davis*, 533 P.2d 222, 234 (Cal. 1975).

The California Online Privacy Protection Act requires commercial websites that collect personally identifiable information⁴³⁰ from consumers to post a conspicuous privacy policy that identifies what information is collected, with whom the information may be shared, and how the consumer can review and request changes to the information, among other requirements.⁴³¹ Thus, any researcher who maintains a commercial website and uses that website to collect real world information about virtual world inhabitants (for example, web surveys posted to a publicly available commercial website) must comply with OPPA, since most researchers have significant contacts with California and almost any researcher will gather data from at least some California consumers. It is unlikely that the researchers would be deemed operators of “commercial” websites.⁴³² Likewise, it is unlikely that research subjects would be deemed “consumers” under the statute.⁴³³ Still, a researcher could fall within these definitions if the researcher was working in conjunction with a commercial entity to create a joint platform for research and commerce—for example, a game designed for profit, but also intended as a research platform.

The issue of fully informed consent is especially important because many TOS and privacy policies are governed by California law. California law is particularly protective of consumers who enter into online standardized electronic contracts that a court considers to be one-sided or to contain surprising terms.⁴³⁴ Thus, California courts may find that the contracts laid out in the privacy policy and the terms of use are simply not enforceable or do not provide sufficient opportunity for informed consent. It is therefore important that the terms of use and privacy policy fully inform users of how their information will be used. As detailed below, I recommend the use of a mandatory pop-up clickthrough agreement that requires the user to check a box next to the consent portion of the document.

430. See PROSKAUER ON PRIVACY, *supra* note 397, § 5:2.1[A] (citing CAL. BUS. & PROF. CODE § 22577(a) (2006)) (defining personally identifiable information as first and last name, address, e-mail address, telephone number, social security number, or any other information that permits a California consumer to be contacted physically or electronically).

431. See PROSKAUER ON PRIVACY, *supra* note 397, § 5:2.1[A] (citing CAL. BUS. & PROF. CODE § 22577(b) (2006)).

432. See CAL. BUS. & PROF. CODE § 22577(c) (2008) (“The term ‘operator’ means any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes.”).

433. See *id.* § 22577(d) (“The term ‘consumer’ means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.”).

434. See, e.g., *Davis v. O’Melveny & Myers*, 485 F.3d 1066 (9th Cir. 2007); *Nagrampa v. MailCoups, Inc.*, 469 F.3d 1257 (9th Cir. 2006); *Comb v. PayPal, Inc.*, 218 F. Supp. 2d 1165 (N.D. Cal. 2002); *Armendariz v. Found. Health Psychcare Servs., Inc.*, 24 Cal. 4th 83 (2000); *Gutierrez v. Autowest, Inc.*, 114 Cal. App. 4th 77 (2003).

IV. BEST PRACTICES

Researchers must always tailor their methodologies to the specific research query they are investigating as well as to the physical or pseudophysical context in which the research takes place. No single set of best practices can cover all of the potential ethical and legal issues that a human subjects research study can raise. What follows is set of guidelines to follow when developing research methodologies for virtual worlds; it is up to specific research teams and IRBs to responsibly modify these principles to protect human subjects in a given research study.

A. Exclusion or Redaction of Private Messages

The critical question for best practices related to the private communications of nonparticipants is whether such communications should be excluded or redacted. Under the Common Rule, human subjects are subjects about whom an investigator “obtains” individually identifiable private information. Because the practice of obtaining individually identifiable private information constitutes human subjects research (as opposed to actually analyzing such data), this Article concludes that exclusion is superior to redaction, that exclusion is technologically possible and simple, and that redaction should be a remedy for errors, rather than a systematic methodology.

Qualitative virtual worlds researchers who seek to log data “in the wild” should take the following steps to exclude private communications to and from nonparticipants in the study. The flexibility of add-on design allows simple programming fixes to restrict data collection to participant communications. If client-side add-ons are used, they should be designed to guard against the collection of communications between participants and nonparticipants. The research add-on should only log messages to and from other users who have installed the add-on. This ensures that only messages between consenting research participants are captured. The add-on should be connected to an account, not a computer. This precaution prevents nonparticipants from inadvertently using participating machines, thus infecting the data set with private communications not covered by informed consent. Another precaution is to design the add-on to indicate prominently to the user that recording is ongoing. The add-on should have an expiration date so that it times out automatically after the logging period is over, and should indicate to the user that logging has ceased.

To avoid deception issues in qualitative research, participant observers should disclose their research status via a group or guild tag (for example, <Researcher>) and in publicly available profiles. If virtual worlds researchers prominently disclose their research status, other users will be able to adjust their communications and conduct toward the researcher according to their expectations of privacy.

If video logging is performed in a laboratory setting—that is, users log in

from their personal accounts and whatever happens on screen is recorded by the researchers—there is a serious chance they will receive “/tells,” or private messages,⁴³⁵ from nonparticipants who have not consented to message logging. This problem is solved when users in laboratory settings create new accounts and avoid contact with nonparticipant acquaintances while they are subject to laboratory video capture. If the research query requires that users log in from their own accounts while subject to video capture in a laboratory, users should disable or hide private chat on the screen. This is an available option in most virtual world settings.⁴³⁶

Quantitative researchers should follow different best practices to protect the privacy of nonparticipants in their virtual worlds research. Quantitative researchers who collect their own data can tailor research questionnaires to avoid obtaining private information. Directing questions toward participant experiences only and cautioning participants not to provide other users’ private information can limit the data set to communications covered fully by informed consent. Quantitative researchers who rely on data sets gathered by the game gods must be even more careful. To the extent possible, quantitative researchers should ask the game gods to omit any private communications—direct messages, chat logs, etc.—from data sets. If game gods are unwilling or unable to conform to this request, quantitative researchers must take responsibility for redacting any personal communications that get through. As a final measure, and cumulatively with all other best practices, all inadvertently gathered private messages from nonconsenting nonparticipants should be redacted. These communications should not be used even if anonymized.

B. Exclusion of Minors

It may be useful for virtual world researchers to adopt best practices from child protection compliance in other statutory regimes (primarily COPPA compliance). Because child protection regimes are generally more restrictive than the privacy policies agreed to by accepting a given virtual world’s EULA,⁴³⁷ researchers ensure their compliance with applicable law by conforming to the more restrictive standards. COPPA compliance best practices utilize a “no-

435. Commands in virtual worlds follow conventions established under Internet Relay Chat commands (IRC), for example in World of Warcraft, “/t” or “/wt” to send a message followed by the actual message. The forward slash communicates a command in the system, and is followed by a message. A user can specify a particular communication, such as an in-game text message to be private and directed to a particular user or a group.

436. See e.g., *PhanxChat*, WOW INTERFACE, <http://www.wowinterface.com/downloads/info6323-PhanxChat.html> (last visited June 6, 2012).

437. See *Second Life Terms of Service*, *supra* note 39 (“By accepting this Agreement in connection with an Account, you represent that you are at least 13 years of age and you have the legal authority to enter into this Agreement.”). It is easier for virtual world companies to opt out of COPPA by limiting the age of entry, such as in *Second Life*.

clickback” arrangement. A no-clickback arrangement first requests the survey taker’s date of birth. A survey taker who claims to be a minor is unable to proceed with the survey. However, in the context of commercial websites that seek to exclude children in order to avoid the need to comply with COPPA, many minors will simply select the “back” button and will provide a false date of birth. A no-clickback arrangement prevents anyone from the child’s IP address from taking the survey once a minor’s birthdate is given. Although this may lock out some legitimate survey takers, it will increase the chance that Internet survey data is not collected on minors who misrepresent their ages.

Another age verification process is also useful. Researchers can design a gateway protocol, much like a clickwrap EULA, that requires users to complete an eligibility survey before beginning a research study. The most effective protocols ask for age verification in different places in the survey and in different formats. Any response indicating that the survey taker is a minor, and any inconsistency with the other responses on the survey, would lock the user’s address out of the study much in the same way as the no-clickback arrangement described above.

Qualitative researchers are positioned to observe human subjects closely, and as such they can usually make sufficient contact with potential human subjects to independently verify their ages. It is important to remember that even this initial contact could implicate the privacy statutes discussed above; if a researcher e-mails a child of fourteen to independently verify the child’s age, the researcher would have obtained personally identifiable information about that person. It is less problematic to use in-world techniques to verify age.

Quantitative researchers who collect their own information can take full advantage of the no-clickback arrangements described above. Unfortunately, quantitative researchers who rely on information gathered by game gods cannot utilize these precautions. Quantitative researchers of this type should ask the game gods not to turn over data sets for users under the age of consent. If the game gods are unwilling or unable to comply, quantitative researchers must redact minors’ information themselves. Because the lower age threshold (age 13) used by most virtual worlds is below the age of informed consent to research, there will almost certainly be minors (ages 13–17) included in the large data sets. Fortunately, the lower age threshold also gives minor users less incentive to lie about their ages—players aged 13–17 will not be excluded from the game due to age, and thus have little incentive to lie. These minors can then be comfortably excluded from the subsequent researcher’s analysis.

C. Obtaining Adequate Informed Consent

1. Primary Research

Researchers who conduct primary qualitative studies are able to design and implement solid informed consent forms before beginning observation of human

subjects. This method is by far the safest. Still, researchers must take proactive measures to ensure that informed consent is valid. Researchers should decide whether the data they collect might be subject to secondary use by other researchers and note that decision in the informed consent form. They should utilize mandatory clickthrough regimes whenever possible to exclude nonconsenting users from research experiments. They should take care to avoid confrontational situations where a user might feel coerced to accept the terms of the agreement.

2. *Secondary Research*

Researchers using secondary qualitative data sets should ensure that the primary researcher for the data set complied with all necessary informed consent procedures. If the secondary researcher is not convinced this is the case, the researcher should personally obtain informed consents. If this is not possible, the researcher should not use the data.

Researchers using secondary quantitative data sets should follow the same procedures if they obtain data originally collected by fellow researchers subject to the same guidelines. However, some secondary quantitative researchers in virtual worlds obtain data directly from game gods. In this case, there is precious little the researcher can do to ensure adequate informed consent. Therefore, researchers should restrict their data acquisitions to virtual worlds whose EULAs include research-grade informed consents within them, as described below, or should refuse to use individually identifiable private information in the study.

Those virtual world providers who wish to share consumers' information with researchers should update their privacy policy to include full disclosure of how the information will be shared and directly inform their current user base of the change. Data gathered prior to the TOS change should be segregated from data gathered after the change, so that data gathered with the promise that it would not be shared is not in fact shared. Moreover, current best practice for TOSs and EULAs is to use a mandatory clickthrough agreement (preferably with a checkbox next to the relevant consent section) that informs the user of exactly what the user is agreeing to prior to permitting access to the virtual world.⁴³⁸ Any further changes should also be sent to the users, and again require the user to click through a mandatory agreement or else not enter the virtual world.

Even this cautious procedure does not solve the problem of coercion. Users who have invested heavily in their virtual communities will not be able to profit from or keep that investment after the TOS change unless they agree to be human subjects. A useful fix, though perhaps not a likely one, would be to use an

438. See, e.g., *Scherillo v. Dun & Bradstreet, Inc.*, No. 09-cv-1557 (JFB)(ARI), 2010 WL 537805 (E.D.N.Y. Feb. 17, 2010) (enforcing a consumer clickthrough agreement with check box).

account-level flag.⁴³⁹ Game gods could then export only the data pertaining to accounts that had agreed to become human research subjects. Only the information of users who agree to human subjects research would be handed over to researchers for secondary analysis.

D. Respecting In-World Cultural Norms

There is also a risk that an observer unfamiliar with the privacy expectations of a population will pursue the observation into a private area. Exporting privacy regimes from one world to another increases the risk of misreading in-world attitudes about privacy. Expectations of privacy in virtual worlds are context-dependent—what constitutes a private place versus a public place is often a matter of convention, not of easily discernable boundaries. Thus, participant observers who quickly change worlds should spend time before beginning work acculturating themselves to the expectations of privacy displayed by the population they intend to study. For example, it may well be that expectations of privacy in *Dungeons & Dragons Online* are quite different from those in *Second Life*, since the former is a PG-rated environment—it is quite impossible to walk in on an avatar in the nude. Not so in *Second Life*, where the risk of a participant observer intruding on private behavior is a serious possibility.

Along with notions of privacy, virtual worlds facilitate the development of specific notions of trust and disclosure. Researchers acclimating to a virtual world are probably most effective if they merely play the role of user, not researcher. However, this acclimation phase should not be used as the basis for observations or recordings to be used in research. A researcher should fully disclose the researcher's status and agenda, whenever and wherever the researcher is conducting an experiment. Preferably, this will be accomplished by unequivocal, public identification of the researcher. For example, researchers in *Second Life* might include the use of a <Researcher> group tag to indicate that a given avatar is in observation mode.⁴⁴⁰

Further, this notion of acclimatization and caution with respect to in-world norms unique to a given virtual world strongly suggest the use of mixed-methods experiments. It is often extremely useful to blend qualitative research, which can give a sense for norms, trust, privacy expectations, and other important in-world cultural constructions, with quantitative research, which can tease out important

439. An account-level flag would be a selection of either yes or no to research under a user's account settings. The user would flag the user's preference, and this selection would not affect access to the virtual world. If the research selection were placed in the EULA, a user could be locked out of the community, and agreement to research would therefore be coercive. The account-level flag would remove the coercive element inherent in a EULA term, which is antithetical to human subjects research.

440. See MCKEE & PORTER, *supra* note 33, at 122–24 (detailing best practices for ethical participant observation).

truths from the data gathered. Although something of a simplification, one might say that qualitative research can guide, and quantitative research, once appropriately guided, can dig deep. Similarly, once quantitative associations have been uncovered, qualitative research can again provide commonsense testing mechanisms to assist in confirming not *whether* a correlation exists between two data points, but in discovering and articulating *why* that connection exists.

E. Treatment of Avatar Names as Identifiable Private Information or Personally Identifiable Information

Another recurring issue is that avatar names themselves may constitute personally identifiable information. Although the Common Rule itself does not define personally identifiable information, its definition of “identifiable private information” notes that such information must be individually identifiable to, or associated with, the subject’s real-world identity.⁴⁴¹ Federal and state privacy law definitions of personally identifiable information are even broader, and turn on whether the information can be used to make contact with the subject. Although it is unlikely that many researchers will be deemed operators of a “commercial website or online service,”⁴⁴² such that the restrictions of federal and state law restricting the information-gathering practices of such operators (COPPA, for example, or California’s Online Privacy Protection Act, OPPA) would directly apply to researchers’ activities, courts are likely to draw from such laws’ definitions of personally identifiable information in attempting to resolve close cases. COPPA defines personally identifiable information as including “an email address or any other substantially similar identifier that permits direct contact with a person online.”⁴⁴³ California’s Online Privacy Protection Act mirrors the COPPA definition and notes that any information that could lead to the contacting of a person in real life constitutes personally identifiable information.⁴⁴⁴

An avatar name, without more, does not constitute “private information”

441. See 32 C.F.R. § 219.102(f)(2) (2012); 45 C.F.R. § 46.102(f)(2) (2010) (“‘Private information’ includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record). Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects.”).

442. 15 U.S.C. § 6501(2)(A) (2012) (“[W]here such website or online service is operated for commercial purposes . . .”).

443. *Id.* § 6501(8)(A)–(F).

444. See, e.g., CAL. BUS. & PROF. CODE § 22577(a)(6) (2008) (“For the purposes of this chapter, the following definitions apply: (a) The term ‘personally identifiable information’ means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following . . . (6) Any other identifier that permits the physical or online contacting of a specific individual.”).

under the Common Rule, since it is publicly displayed. If the avatar's underlying identity was discoverable or if the information was associated with the subject's real-world identity, the avatar identity would be treated as private information under the Common Rule. On the other hand, pure "screen names" that are unconnected with "any individually identifiable information" are not considered personally identifiable information for COPPA purposes.⁴⁴⁵ It is therefore not at all clear whether an avatar fits more closely the FTC's concept of a "screen name," or is closer to a Facebook name, Skype name, Twitter name, or e-mail address, all of which do constitute personally identifiable information.⁴⁴⁶ There is no bright line between a screen name and, for example, an instant messaging handle. The primary criterion seems to be how familiar adjudicators are with the technology that permits contacting the subject. An avatar name is a means by which a citizen can be contacted in real life. Indeed, an avatar name is better than an e-mail address for purposes of contacting a gamer. In Second Life, an avatar name is often directly linked to an e-mail address, such that messages to the avatar are automatically sent to e-mail.⁴⁴⁷ Further, in certain virtual worlds, like IMVU,⁴⁴⁸ the line blurs completely: the avatar name *is* an instant messaging handle, and thus falls directly under the definition of personal information.

Although this area of law is unsettled, best practices trend in favor of treating avatar names as personally identifiable information. First, virtual world denizens routinely associate their avatars with their real world identities, both in virtual

445. See PROSKAUER ON PRIVACY, *supra* note 397, § 11:3.2; see also Final Rule Notice, 64 Fed. Reg. 59,888, 59,892 & n.66 (Nov. 3, 1999) (codified at 16 C.F.R. pt. 312) ("Several commenters sought further guidance on whether the use of screen names would trigger the Act's requirements. If a screen name is not associated with any individually identifiable information, it is not considered 'personal information' under this Rule One commenter also asked whether operators would be required to ensure that a screen name chosen by a child did not contain individually identifiable information. TRUSTe (Comment 97) at 3. Operators do not have a specific duty to investigate whether a screen name contains such information. However, an operator could give children warnings about including such information in screen names, especially those that will be disclosed in a public forum such as a chat room.").

446. See Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,891 & n.49 (1999) ("The Commission received several comments regarding the definition of 'online contact information.' One commenter suggested that the Commission include in the definition such identifiers as instant messaging user identifiers, which are increasingly being used for communicating online. The Commission believes that these identifiers already fall within the proposed definition, which includes 'any other substantially similar identifier that permits direct contact with a person online.' After reviewing the comments, the Commission has determined that no changes to this definition are necessary Another example of 'online contact information' could be a screen name that also serves as an e-mail address.").

447. See *Instant Messages*, SECOND LIFE, <http://community.secondlife.com/t5/English-Knowledge-Base/Instant-messages/ta-p/700089> (last visited June 6, 2012) ("Instant messages (IMs) can be emailed to you offline at the email address in your Second Life contact information. This feature can be useful to Second Life business owners, socialites, or anyone else who needs to be able to respond to IMs when they are not inworld.").

448. See IMVU, <http://www.imvu.com> (a virtual world where users create three-dimensional avatars and communicate directly to one another with avatar names).

worlds and in real-world social forums. Second, virtual worlds users tend to keep persistent handles, or identities, across multiple different worlds. This is useful for the user precisely because it permits the user's friends to renew acquaintances once a social group migrates into a new world. Gamers also use avatar names as e-mail addresses and IM handles, and messages to avatars are often automatically forwarded to e-mail accounts. But most importantly, virtual world users have valuable reputations associated with the avatar name itself. Avatar names are made to be recognizable; a friend, guildmate, or even casual in-world acquaintance of the virtual world user will know who a given avatar is. Those relationships and reputations may be damaged if the study participant is identified, especially if studies take inadequate precautions to exclude nonparticipant communications. In such a case the subject's involvement in the study would precipitate the nonconsensual involvement of the subject's social circle.

F. Anonymization of Personally Identifiable Information for International Transport

Research teams with an international collaborative component may wish to design their research protocols to benefit from the anonymization exception within the European Union Data Privacy Directive.⁴⁴⁹ The Data Privacy Directive prohibits the movement of citizens' personal data to other countries that have less stringent data protections than those offered by the Directive.⁴⁵⁰ There are three exceptions to the Directive. Data may be anonymized,⁴⁵¹ data exporters may seek the full informed consent of the persons to whom the data relates,⁴⁵² or companies may seek "safe harbor" status by promising to abide by the European Union's rules.⁴⁵³

If researchers choose to take advantage of the anonymization exception, they must be thorough. As evidenced by the nominally anonymized AOL search data set and the Blockbuster/Facebook Beacon data set, removing immediately identifiable information is not enough. Researchers must remove relational identifiers as well. One method of doing this is to remove data values that contain information unique enough to identify individuals or groups.⁴⁵⁴ Another potential technique is the mathematical "jittering" of data, which injects enough uncertainty to make individual identification impossible but not enough to affect analysis of

449. PROSKAUER ON PRIVACY, *supra* note 397, §14:2 (citing Directive, *supra* note 406). It is worth noting that the Directive itself is not the law that directly governs data transport; rather, it requires each of the twenty-seven members to which it is directed to "transpose" or implement local laws embodying its thrust.

450. See PROSKAUER ON PRIVACY, *supra* note 397.

451. See *id.* § 14:3.1.

452. See Directive, *supra* note 406, at ch. IV, art. 26.

453. See PROSKAUER ON PRIVACY, *supra* note 397, § 14:3.2.

454. See Margaret Law, *Reduce, Reuse, Recycle: Issues in the Secondary Use of Research Data*, IASSIST Q., Spring 2005, at 5, 8.

large amounts of data.⁴⁵⁵ These methods could be very well suited to massive virtual worlds data sets.

G. Diversifying the Research Pool of Virtual Worlds

Demographic imbalances are to some degree inherent in virtual worlds. But there are ways to mitigate any imbalances. Too many virtual worlds studies focus on Second Life and World of Warcraft. The difficulty is that those worlds contain very specific (although different) demographic mixes. For example, World of Warcraft is a standard sword-and-sorcery video game focusing on loot acquisition, advancement, and combat; population figures are heavily male. Second Life has a more balanced male-to-female ratio, but use of Second Life for research purposes is still problematic because the world is so unique among virtual worlds, and because it represents a tiny subfraction of the hundreds of millions of users of virtual worlds. It is possible—and desirable—to conduct experiments in virtual worlds that cater to a demographic other than the standard young and male group. Faunasphere was one virtual world that had drawn a close-knit community of middle-aged to older women. Including virtual worlds like Faunasphere in research would do much to more equitably distribute the benefits of virtual worlds research.

Researchers can address digital divide concerns⁴⁵⁶ by focusing research less on the high-end graphics and bandwidth-intensive virtual worlds like Second Life and World of Warcraft. Instead, researchers should structure studies on the far larger, lower bandwidth, and more inclusive virtual worlds like Habbo Hotel and Coke Studios. In so doing, researchers would be serving a broader population as well as increasing the relevance and accuracy of their findings. Of course researchers need not abandon Second Life and World of Warcraft entirely; as broadband access becomes more widespread and high-end graphics cards become less expensive, digital divide concerns will not be so problematic.

H. Educating and Working With IRBs

Greg Koski, former director of OHRP, called the recent increase in stringent IRB reviews “reactive hyper-protectionism.”⁴⁵⁷ Unfortunately, the phenomenon sometimes leads to an oppositional tension between IRBs and researchers.⁴⁵⁸

455. *See id.* at 9.

456. The “digital divide” refers to the effects of economic opportunity to access information services. *See generally* Peter K. Yu, *Foreword: Bridging the Digital Divide: Equality in the Information Age*, 20 CARDOZO ARTS & ENT. L.J. 1 (2002).

457. Tooher, *supra* note 165.

458. *See* Bernard A. Schwetz, *Protecting Subjects Without Hampering Research Progress: Guidance from the Office for Human Research Protections*, 74 CLEV. CLINIC J. MED. S60, S61 (2007) (describing “antagonism” as “an obstacle in itself, getting in the way of solving the problems and moving the protocol through.”).

Another former OHRP director, Bernard Schwetz, noted “[t]he purpose of guidance is to allow for flexibility in appropriate circumstances.”⁴⁵⁹ IRBs should remember that federal regulations are designed broadly and should be tailored to each specific experiment. Federal guidance that makes sense for a biomedical project proposal may be preposterous when applied to a virtual worlds project proposal, and vice versa.

Another common problem with IRB review is lack of expertise.⁴⁶⁰ Federal regulations allow IRBs to bring in outside experts to help them examine methodologies dealing with topics and populations with which they are unfamiliar. Researchers should act as facilitators for this process, offering the names of experts the IRB may wish to invite into the decision-making process. A well-informed IRB will better understand the ethical issues unique to virtual worlds research and will be able to issue strong recommendations to improve an inadequate proposal. It will also be able to approve adequate virtual worlds research proposals with more confidence, avoiding the overly stringent “reactive hyper-protectionism” Koski warns against.

I. Using Add-Ons and Scrapers Effectively and Appropriately

Researchers who seek to use add-ons and scrapers should secure the consent of the virtual world provider where doing so is practical. Choosing well-designed codes with minimal impact on game play and working to minimize the load that add-ons and scrapers place on game and web servers will make the research tools more palatable to game developers. Researchers should also ensure that add-ons comply with all elements of a virtual world’s UI add-on development policy and EULA. Finally, they should have a contingency plan for removal of locally run add-ons if a game god determines that such add-ons negatively impact gameplay. Quick and thorough removal of any offending add-ons will help preserve game developers’ relationship with the research community so that virtual worlds can continue to be a viable option for conducting studies.

V. CONCLUSION

There is a tension at the center of virtual worlds human subjects research. Researchers know that virtual worlds users care deeply about their online identities, property, reputations, and relationships. At the same time, however, some commonly used research methodologies put those relationships at risk.

459. *See id.* (Schwetz goes on to admit that IRBs who treat guidance as mandate can negatively impact research: “If an IRB spends too much of its time on tasks that are not mandated, it may not devote enough attention to its real work, which not only might contribute to research delays but may jeopardize the safety of research subjects.”).

460. *See id.* (“Lack of expertise among IRB members is often the primary problem. A common mistake committed by inexperienced IRB members is to send protocols back to investigators for revision without providing specific directions to resolve the issues.”).

There is an overarching sense that virtual worlds are not truly “real,” and so the cost of losing virtual reputations, relationships, or property is not as great as in the real world. Researchers are too often willing to condone the use of methodologies that they would not use if the experiment exposed human subjects to similar losses of property, community, or reputation in real life. If researchers fail to take the very real nature of virtual worlds into account, they risk compromising their own ethics as well as skirting applicable law.

There are solutions. While virtual worlds do present novel challenges, they also offer new affordances for securing adequate informed consent from research subjects, for gathering rich data sets, and for protecting subject privacy. With some knowledge about how specific virtual worlds work and how technology can be used to protect instead of compromise privacy interests, researchers can meet the highest ethical and legal standards for conducting virtual worlds research.