

PRIVACY AND THE NEW VIRTUALISM

JONATHON W. PENNEY*

10 YALE J.L. & TECH. 194 (2008)

ABSTRACT

First generation cyberlaw scholars were deeply influenced by the uniqueness of cyberspace, and believed its technology and scope meant it could not be controlled by any government. Few still ascribe to this utopian vision. However, there is now a growing body of second generation cyberlaw scholarship that speaks not only to the differential character of cyberspace, but also analyzes legal norms within virtual spaces while drawing connections to our experience in real space. I call this the New Virtualism. Situated within this emerging scholarship, this Article offers a new approach to privacy in cyberspace by drawing on what Orin Kerr calls the internalist or virtualist perspective. The virtualist approach to privacy in cyberspace shifts the focus away from the concept of privacy itself, which has been over-theorized and over-categorized by privacy theorists, to analyzing and theorizing persons in cyberspace and how they ought to be understood. It focuses on virtual persons and the distinct privacy concerns they raise, and reconnects ideas about informational and data privacy to traditional normative justifications for privacy based on personhood. Adopting a virtualist approach to privacy in cyberspace has conceptual, normative, constitutional, and public policy benefits.

* Recently a postgraduate researcher at the Faculty of Law, Oxford University, where he was a Mackenzie King Travelling Scholar. The author would like to thank the staff of the Oxford Internet Institute for their patience and assistance in the course of this research and YJoLT editor Caitlin Hall for her help in preparing the article for publication. He would also like to thank Robert Danay, Jonathan Zittrain, Richard Albert, Ali Abrar,, Julie Cohen, and Kandia Aird for their advice, comments and/or suggestions.

TABLE OF CONTENTS

I. Introduction..... 196

II. The New Virtualism: A Brief History..... 200

 A. The Original Virtualists 200

 B. From the Old to New 201

III. Privacy’s Discontent: Cyberspace 205

 A. The Present Situation 205

 B. The Intellectual Origins of the Problem: *Whalen v. Roe* and the
Externalist Perspective 210

IV. A Virtualist Account of Privacy in Cyberspace 214

 A. Personhood in Cyberspace..... 216

 B. Conceptualizing Virtualist Privacy 229

V. Why Virtualist Privacy? 235

 A. Normative and Conceptual Advantage..... 235

 B. Virtualist Privacy and the Constitution 240

 C. Virtualist Privacy, Public Policy, and Code 244

VI. Moving Forward: Virtualist Privacy in America and Abroad..... 248

I. INTRODUCTION

In his *Declaration of the Independence of Cyberspace*, John Perry Barlow famously pronounced the existence of a new frontier called “cyberspace,” a world altogether distinct from real space. From this premise of difference and electronic independence, Barlow concluded that cyberspace would remain “immune” from the “sovereignty” of traditional governments.¹ The simplicity and revolutionary character of these ideas was appealing—so appealing that many early “cyberlaw” scholars² followed Barlow to argue that traditional laws ought not apply to the virtual worlds of cyberspace, that they be left alone to formulate their own legal rules and norms.³

Many have since questioned the “cyberutopian vision” of cyberspace as existing beyond the reach of traditional laws and forms of governance.⁴ Recently, John L. Goldsmith and Tim Wu offered a sound debunking of Barlow’s claim, demonstrating that traditional governments do, in many ways, control cyberspace.⁵ The strength of their arguments led Orin Kerr to remark that few still take the

¹ John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), reprinted in CRYPTO ANARCHY, CYBERSTATES, AND PIRATE UTOPIAS 27, 28 (Peter Ludlow ed., 2001), available at <http://www.eff.org/~barlow/Declaration-Final.html>.

² See Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

³ See, e.g., I. Trotter Hardy, *The Proper Legal Regime for “Cyberspace,”* 55 U. PITT. L. REV. 993, 994, 1019-25 (1994) (advocating self-help, custom, and contract to regulate cyberspace); David R. Johnson & David G Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367-75 (1996) [hereinafter Johnson & Post, *Law and Borders*] (noting possibilities of internal regulation of Internet through competing rule sets); David R. Johnson & David G Post, *And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law*, in COORDINATING THE INTERNET 62, 65 (Brian Kahin & James H. Keller eds., 1997) [hereinafter Johnson & Post, *Meditation*] (arguing for a decentralized system of Internet governance); Henry H. Perritt, Jr., *Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?*, 12 BERKELEY TECH. L.J. 413, 419-20 (1997) (contending that as a general rule “self-governance is desirable for electronic communities”); David G Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155, 161 (1996) (arguing for metaphor of cyberspace as separate space); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 912-917 (1996) [hereinafter Reidenberg, *Governing*] (arguing that attempts to define rules for the development of cyberspace rely on disintegrating concepts of territory and sector, and ignore the new borders that transcend national boundaries); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) [hereinafter Reidenberg, *Lex Informatica*] (arguing for a “Lex Informatica” which would regulate cyberspace through technological devices).

⁴ Orin S. Kerr, *Enforcing Law Online*, 74 U. CHI. L. REV. 745, 745 (2007).

⁵ See JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006); Kerr, *supra* note 5, at 751-52.

cyberutopians “seriously,”⁶ and to the extent that such views do remain influential, Goldsmith and Wu have offered a decisive rebuke.

It is now common to speak of first and second generation cyberlaw scholarship.⁷ The first generation cyberlaw scholars, deeply influenced by Barlow and the cyberutopians, were wrong about how “free” the internet and cyberspace would be from the arm of the state. But this does not mean we should completely discard all ideas in this early body of scholarship, nor the *Declaration* itself. It spoke to much more than a thesis about limited government; it spoke first and foremost to the differential character of cyberspace and its virtual worlds. Entering cyberspace meant entering someplace different, inhabited not by real people, but our “virtual selves.”⁸ As Lawrence Lessig has persuasively shown, there *is* something different about cyberspace and virtual worlds, and the laws and norms that govern them.⁹ Early scholars who wrote of cyberspace as a separate world beyond real space have been aptly called the “virtualists” by James Grimmelman.¹⁰ So while Barlow and early virtualists were wrong about the independence of cyberspace, they did offer an important perspective about the uniqueness of cyberspace and how it might impact cyberlaw problems.

Building upon these earlier ideas, a new body of virtualist scholarship is emerging.¹¹ I call this the New Virtualism. The difference between this scholarship, and what Jack Balkin calls “first generation” cyberlaw scholarship,¹² is that the New Virtualism, while exploring the legal and technological implications of cyberspace and virtual worlds as places distinct from real space, forgoes the cyberutopian dream that cyberspace can or will be a self-governing domain, independent of the laws of territorial governments.¹³ Instead, the New Virtualism consciously negotiates the “borders” between cyber and real space, drawing parallels and connections in order to better understand how law can and should work in virtual landscapes.

The New Virtualism also confronts what Orin Kerr calls the problem of “internal” and “external,” or real and virtual, perspectives

⁶ Kerr, *supra* note 5, at 751.

⁷ E.g. LAWRENCE LESSIG, *CODE VERSION 2.0*, at xiv-xv (2006); Jack Balkin, *Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds*, 90 VA. L. REV. 2043, 2044 n.3 (2004); Paul Schiff Berman, *Cyberspace and the State Regulation Debate: The Cultural Value of Applying Constitutional Norms to “Private” Regulation*, 71 U. COLO. L. REV. 1263, 1264-65 (2000).

⁸ Barlow, *supra* note 2.

⁹ LESSIG, *supra* note 8.

¹⁰ James Grimmelman, *Virtual Borders: The Interdependence of Real and Virtual Worlds*, FIRST MONDAY (Feb. 6, 2006), http://www.firstmonday.org/issues/issue11_2/grimmelman/index.html.

¹¹ See *infra* note 36.

¹² Balkin, *supra* note 7, at 2044 n.3

¹³ Johnson & Post, *Law and Borders*, *supra* note 3.

of cyberlaw,¹⁴ but unlike original virtualism, it does not view them in all-or-nothing fashion. An internal or “virtualist” perspective means approaching cyberlaw problems from the perspective of a person *internal* to the virtual world or reality created in the “world of cyberspace.”¹⁵ That is, it approaches the person as someone inhabiting virtual worlds, not in physical form, but as an identity that is negotiating the virtual terrain of cyberspace. The external or real perspective approaches the “internet user” as simply someone sitting at a computer, very much in the real world and its real space.¹⁶ The original virtualists embraced the “internal” or virtual perspective, claiming that the distinctive character of cyberspace rendered traditional laws—those conceived in real space from an external perspective—irrelevant.

In contrast, the New Virtualism understands that the borders between cyberspace and real space are not clearly defined.¹⁷ They are porous, flexible, fluid, and shifting. Thus, it explores legal questions from an internal perspective, but recognizes that, in some instances, an external perspective is warranted to fully understand the law and how it ought to work in cyberspace. The New Virtualism, like its forebearer, heralds the uniqueness and importance of cyberspace and virtual worlds, but rather than ignoring the impact of realism and the laws of real space, draws them into the analysis, offering a deeper level of analysis for cyberlaw’s deepest questions.

This Article attempts to bring this approach to the concepts of privacy and personhood in cyberspace. My argument is simple. The present predominant approach to privacy in cyberspace—based mainly on the concept of information privacy—has failed to make headway against privacy threats because it has relied too heavily on an implicit realist or external perspective. Information privacy conceives of the person sitting at their computer, external to cyberspace, with information *about them* collected, moved, stored, and existing in remote places, be it electronic databases, computers, or other private actors or electronic media in networks. Questions and issues about the identity of the person in cyberspace and how this personal information relates to their “self” in cyberspace are completely precluded by the idea of information privacy. Since information privacy conceives of information cut off from the person, it fails to account for the important ways privacy in this information affects *personhood* in cyberspace, our liberty and ability to achieve self-determination in virtual worlds.

Instead, we must ask different questions. The virtualist approach to privacy in cyberspace shifts the focus the away from the concept of privacy itself, which has been over-theorized and over-

¹⁴ Orin Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 357-405 (2003).

¹⁵ *Id.* at 357.

¹⁶ *Id.*

¹⁷ See Balkin, *supra* note 7, at 2060.

categorized by privacy theorists, to analyzing and theorizing persons in cyberspace and how they ought to be understood. It focuses on virtual persons and their privacy interests and issues, and reconnects ideas about informational and data privacy to more fundamental normative justifications for privacy based on personhood. I set out these ideas in Part IV (after a survey of the present state of privacy scholarship in Part III) and argue, among other things, that data information is constitutive of personhood in cyberspace in a much more fundamental way than in real space. That is, unlike privacy in the real world, where we have physical bodies separate from the information recorded about us, personhood in cyberspace is more intimately connected to this information. If privacy sets out to protect the interests of the *virtual person* in cyberspace, then privacy in this data and information becomes essential. To be clear, I do not suggest that virtual persons are somehow removed from our actual selves in real space, and thus have independent privacy interests. Rather, our “virtual person” is an important extension of our own person and identity, with implications for intimacy and dignity. Virtualist privacy offers the best means to address these issues.

Part V outlines the advantages of a virtualist approach to privacy in cyberspace. The first is conceptual and normative. It clarifies that informational privacy is not a separate subset of privacy, but a manifestation of traditional understanding of privacy tied to personhood. Privacy ought not be further complicated, but simply understood from a virtualist perspective in cyberspace. This, I will argue, simplifies the concept of privacy and its taxonomy while reconnecting privacy in cyberspace to stronger normative justifications relating to personhood. The second advantage is constitutional. I will argue that a virtualist approach offers a new basis to found a broader constitutional right, or constitutional commitment, to informational privacy in cyberspace. A constitutional commitment to informational privacy is important not only for traditional reasons—to protect people from government—but also offers a normative framework to encourage both state and non-state actors to take more proactive measures to protect privacy.

The third advantage relates to public policy and code. I respond to skeptics to suggest that recognition of a clear constitutional commitment to broad informational privacy protection in cyberspace would be irrelevant as many privacy threats originate from private actors. I argue that a constitutional commitment imposes additional responsibilities on both state and private actors and can help foster a constitutional culture of privacy necessary for robust privacy protection now and in the future. Moving beyond constitutional arguments, I suggest that virtualist privacy, which speaks to experiences of living and learning in virtual worlds, can help influence the next generation of programmers who will be responsible for shaping the future of cyberspace and the values hardwired into its code. This generation will have experienced and lived virtual worlds in greater depth than any before it, and our thinking on things like privacy

and other important values needs to keep up. The virtualist perspective is part of this shift in ideas.

II. THE NEW VIRTUALISM: A BRIEF HISTORY

A. THE ORIGINAL VIRTUALISTS

The original virtualists had a clearly defined project for cyberspace. These “first generation” cyberlaw scholars urged lawmakers to leave cyberspace alone and let it “produce its own rule sets” to govern itself.¹⁸ This idea echoed those of the early “cyberutopians”¹⁹ like John Perry Barlow and Julian Dibbell, who heralded the liberating properties of cyberspace and virtual reality.²⁰ The techno-libertarian philosophy of Barlow and Dibbell, with its unwavering promotion of the ideals of liberty and free speech, was a philosophy shared by the many programmers and developers who helped found and shape the Internet—and thus cyberspace itself—in its early years.²¹ So when governments began paying more attention to activities in cyberspace, an important question was posed: Who would be responsible for regulating cyberspace? The answer from Barlow and Dibbell was clear. Governments had no role to play. Cyberspace existed beyond the reach of the state, as a place without jurisdictional borders or national laws. Traditional governments would “have no sovereignty.”²²

Early cyberlaw scholars, whom we might also call the original virtualists, would answer this question similarly. They too believed there was something “uniquely valuable” about virtual worlds and cyberspace, something “worth nurturing.”²³ But rather than offer a radical libertarian philosophy in the vein of Barlow and Dibbell, the

¹⁸ *Id.* at 2044 n.3 (“[T]he first generation of cyberlaw scholarship . . . urged courts and legislatures to treat the Internet as a separate space or series of spaces that could produce its own rule sets.”).

¹⁹ I borrow “cyberutopian” from Orin Kerr, *supra* note 4, at 751. Fred Turner uses the term “techno-utopians.” FRED TURNER, FROM COUNTERCULTURE TO CYBERCULTURE: STEWART BRAND, THE WHOLE EARTH NETWORK, AND THE RISE OF DIGITAL UTOPIANISM 261 (2006).

²⁰ See Barlow, *supra* note 1; see also Julian Dibbell, *A Rape in Cyberspace: How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society*, VILLAGE VOICE 38 (Dec. 21, 1993) (describing how a virtual Internet community reacted to an unruly participant by creating a self-governance scheme).

²¹ See, e.g., GOLDSMITH & WU, *supra* note 5, at 10, 13, 24-25 (writing that Dibbell and Barlow created “a new frontier, where people lived in peace, under their own rules, liberated from the constraints of an oppressive society and free from government meddling” and that this vision was shared by other pioneers of cyberspace who believed “the Internet might transcend territorial law and render the nation-state obsolete”); see also TURNER, *supra* note 19, at 261 (writing that the “techno-utopians” had “conjured up visions of a disembodied, peer-to-peer utopia . . . a return to a more natural, more intimate state of being”).

²² Barlow, *supra* note 1.

²³ Grimmelmann, *supra* note 10.

original virtualists formulated creative cyberlaw solutions for how virtual communities and worlds might govern themselves, often incorporating technological as well as legal proposals.²⁴ A classic statement of original virtualism is the seminal article “Law and Borders — The Rise of Law in Cyberspace”²⁵ published in the *Stanford Law Review* by David Johnson and David Post in 1996. Johnson and Post heralded the “special character” of cyberspace, and advocated that traditional laws should not apply to it, or in the least, ought to have limited application.²⁶ As an alternative to the territorial laws of the state, Johnson and Post offered rule sets based on community consensus.²⁷

The original virtualists also took sides. Because they believed in the special character of cyberspace, and theorized it as a separate place, they fully embraced the “internal” or virtualist perspective. The external or realist perspective was something inextricably tied to the laws and systems of control exercised by territorial governments, and the old ways of thinking about law and virtual worlds. That type of thinking had to be discarded in order to ensure that the new laws that would govern cyberspace and virtual worlds would take into account the “special characteristics” of these cyberspaces, and the “persons, places, and things found there.”²⁸ Those people *local* to cyberspaces, that is, those living *within* these virtual communities, would have the best ideas about how to regulate them.

B. FROM THE OLD TO NEW

As Internet use and cyberspace continued to migrate toward mainstream popular culture in the late 1990s, two important things became clear. First, cyberspace was not as independent as the virtualists and cyberutopians had hoped. Cyberspace could not guarantee liberty and freedom. Rather, these ideals depended upon

²⁴ See Hardy, *supra* note 3, at 1019-25 (advocating self-help, custom, and contract to regulate cyberspace); Johnson & Post, *Meditation*, *supra* note 3 (arguing for a decentralized system of Internet governance); Johnson & Post, *Law and Borders*, *supra* note 3, at 1367-75 (noting possibilities of internal regulation of the Internet through competing rule sets); Perritt, *supra* note 3, at 419-20 (contending that as a general rule “self-governance is desirable for electronic communities”); Post, *supra* note 3, at 161 (arguing for metaphor of cyberspace as separate space); Reidenberg, *Lex Informatica*, *supra* note 4 (arguing for a “Lex Informatica” which would regulate cyberspace through technological devices); Edward J. Valauskas, *Lex Networkia: Understanding the Internet Community*, FIRST MONDAY (Oct. 7, 1996), <http://www.firstmonday.dk/issues/issue4/valauskas/index.html> (calling for formalization of Internet self-governance).

²⁵ Johnson & Post, *Law and Borders*, *supra* note 3.

²⁶ *Id.* at 1400-01 (writing that the “new law” created in cyberspace be treated as a “distinct doctrine, applicable to a clearly demarcated sphere, created primarily by legitimate, self-regulatory processes, and entitled to appropriate deference”).

²⁷ See *id.* at 1401.

²⁸ *Id.*; see also Reidenberg, *Governing*, *supra* note 3 (arguing that attempts to define rules for the development of cyberspace rely on disintegrating concepts of territory and sector, and ignore the new borders that transcend national boundaries).

code and design. Lawrence Lessig popularized these ideas with his influential pun “code is law.”²⁹ Like law, code reflects certain values, but there is nothing inherent in code that secures freedom or liberty. The liberty and autonomy that seemed so “fundamental” and unique to cyberspace really were not fundamental at all.³⁰ Second, the borders between cyberspace and real space were not as clearly defined as the original virtualists presumed.³¹ Increased commodification was slowly eroding the seeming immutable borders of the virtual and real.³² Moreover, despite the predictions of the cyberutopians, traditional territorial governments had become important players in Internet governance.³³ The external arm of the state could reach into the virtual realm of cyberspace after all. Ten years after the publication of “Law and Borders,” Johnson and Post remarked that while in some ways the boundaries between real space and cyberspace are clearer, in others they are “becoming more and more permeable each day.”³⁴

These developments showed that the first generation cyberlaw scholars had missed the mark. Things were more complicated than they had assumed. But this did not mean that the skeptics of cyberlaw were right, that cyberlaw had nothing original to say.³⁵ A more flexible approach to these sorts of cyberlaw questions was required, but the interesting legal, theoretical, and normative issues in cyberlaw, like the question of perspective discussed above, would not go away. They deserved further exploration.

Today, a new body of cyberlaw scholarship is emerging to take up this challenge. This body of work I have called the New Virtualism. The scholarship is still *virtualist* in that like the earlier scholarship, it often analyzes cyberlaw issues from an internal or virtualist perspective. But this work is “new” in that it differs in important ways from original virtualism. First, the New Virtualism, like the original, heralds the uniqueness of cyberspace and virtual worlds, but offers a

²⁹ LESSIG, *supra* note 7, at 5.

³⁰ LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 6 (1999) (“Values that we now consider fundamental will not necessarily remain. Freedoms that were foundational will slowly disappear.”).

³¹ See TURNER, *supra* note 19, at 260-61 (writing that the “rhetoric” of the utopians neglected the important material and technological connections between the Internet and the real world).

³² See Balkin, *supra* note 7, at 2059 (arguing that real-world commodification is causing the breakdown between game spaces and real space).

³³ See generally GOLDSMITH & WU, *supra* note 5.

³⁴ David Johnson & David Post, *The Great Debate: Law in the Virtual World*, FIRST MONDAY (Feb. 6, 2006), http://www.firstmonday.org/issues/issue11_2/post/index.html.

³⁵ See, e.g., Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, U. CHI. LEGAL. F. 207, 208 (1996) (arguing that cyberlaw is simply law involving technology); Christopher M. Kelly, *The Cyberspace Separatism Fallacy*, 34 TEX. INT’L. L.J. 413, 418 (1999) (making a similar argument in conclusion); Joseph H. Sommer, *Against Cyberlaw*, 15 BERKELEY TECH. L.J. 1145, 1147 (2000) (arguing cyberlaw is “nonexistent”).

more flexible and fluid approach. Drawing insight from developments since the early 1990s, rather than proclaiming or advocating the independence of cyberspace, the New Virtualism explores how real and virtual worlds interact, drawing connections, analogies, and parallels between real and virtual spaces.³⁶ The realization that the borders between real space and cyberspace are not clearly drawn does not mean cyberlaw writers must fall silent. Rather, this reality raises new, interesting questions about how law works, or ought to work, in virtual spaces. Jack Balkin's work on "virtual liberty"³⁷ and James Grimmelmann's exploration of the "interdependence" of real and virtual worlds³⁸ and comparative virtualism,³⁹ are good examples of such inquiries.

³⁶ See James Grimmelmann, *Virtual Power Politics*, in *THE STATE OF PLAY: LAW, GAMES, AND VIRTUAL WORLDS* (Jack M. Balkin & Beth S. Noveck eds., 2006) (exploring software design through lens of virtual world politics); Balkin, *supra* note 7 (discussing "virtual liberty" in virtual worlds and the boundaries between cyberspace and real space); see also Richard H. Bartle, *Why Governments Aren't Gods and Gods Aren't Governments*, *FIRST MONDAY* (Sept. 2006), http://www.firstmonday.org/issues/special11_9/bartle/ (calling for formalization of Internet self-governance); Richard A. Bartle, *Virtual Worldliness: What the Imaginary Asks of the Real*, 49 *N.Y.L. SCH. L. REV.* 19 (2005); Edward Castronova, *The Right to Play*, 49 *N.Y.L. SCH. L. REV.* 185, 185, 209-10 (2005) (writing that virtual worlds "represent a new technology" allowing "deeper and richer access to the mental states" and exploring how a "right to play" can be preserved in the face of real world concerns and the hierarchies of "ordinary human affairs"); Grimmelmann, *supra* note 10 (comparing virtualist and realist perspectives in cyberlaw and emphasizing the importance of recognizing the interconnectedness of both, to preserve the distinctiveness of cyberspaces); James Grimmelmann, *Virtual Worlds as Comparative Law*, 47 *N.Y.L. SCH. L. REV.* 147 (2004) [hereinafter Grimmelmann, *Virtual Worlds*] (approaching the law within virtual worlds as comparative legal study); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 *CAL. L. REV.* 439 (2003) (arguing that the metaphor of cyberspace legitimizes the imposition of private property-like regimes on virtual spaces, precluding their common use and enjoyment); Kerr, *supra* note 14 (exploring the "problem of perspective" in cyberlaw); F. Gregory Lastowka & Dan Hunter, *The Laws of the Virtual World*, 92 *CAL. L. REV.* 1 (2004) [hereinafter Lastowka & Hunter, *Virtual World*] (arguing that items in virtual worlds ought to have property protection as much as items in non-virtual worlds); F. Gregory Lastowka & Dan Hunter, *Virtual Crimes*, 49 *N.Y.L. SCH. L. REV.* 293 (2004) (exploring whether destruction of virtual property can or ought to be conceived as criminal activity); Beth Noveck, *The State of Play*, 49 *N.Y.L. SCH. L. REV.* 1 (2004) (discussing questions raised by virtual worlds for real world laws); Tal Zarsky, *Information Privacy in Virtual Worlds: Identifying Unique Concerns Beyond the Online and Offline Worlds*, 49 *N.Y.L. SCH. L. REV.* 231 (2004) (discussing possible questions raised by virtual worlds for real world laws); Edward Castronova, *Theory of the Avatar* (CESifo Working Paper Series, Working Paper No. 863, 2003) (exploring human activity in virtual worlds through bodily representation in avatar form); Edward Castronova, *On Virtual Economies* (CESifo Working Paper Series, Working Paper No. 752, 2002) [hereinafter Castronova, *Virtual Economies*] (exploring the growth of virtual economies and the impact on real world economies); Edward Castronova, *Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier* (CESifo Working Paper Series, Working Paper No. 618, 2001) (conducting an economic analysis of Sony's EverQuest virtual world called "Norrath").

³⁷ Balkin, *supra* note 7.

³⁸ Grimmelmann, *supra* note 10 (comparing virtualist and realist perspectives in

Moreover, the New Virtualism offers a less hierarchical understanding of perspective in cyberlaw issues. The original virtualists implicitly privileged the internal perspective by exploring legal issues, norms and concepts from a viewpoint within cyberspace, while minimizing the importance or relevance of the external perspective. This is not a surprising revelation. The early cyberlaw scholars were grappling with difficult questions of law and technology, and it made sense to approach these questions from *within* the cyberspaces they were analyzing. The New Virtualism, however, while still focusing primarily on the internal or virtualist perspective, does not dismiss externalism, but brings real space concerns into the analysis. Tal Zarsky's recent work on informational privacy in "online and offline worlds"⁴⁰ and Edward Castronova's analysis of "virtual economies,"⁴¹ are examples of work that weave this balance.

Finally, the New Virtualism has embarked on a rich exploration of law in virtual worlds, often incorporating—or, using Lessig's term, "translating"⁴²—real-world legal concepts into the cyber realm. Recent scholarship on the laws of gaming and virtual worlds⁴³ and the groundbreaking work by F. Gregory Lastowka and Dan Hunter on virtual property, are notable here.

I want to situate this Article within this new and still-emerging body of scholarship. As noted, the New Virtualism approaches perspective in cyberlaw in a more flexible way than early cyberlaw scholarship. But moreover, I believe it is possible to transform what Orin Kerr calls the "problem of perspective"⁴⁴ in cyberlaw into a powerful analytical tool. Legal scholars have often failed to recognize the distinction between real and virtual perspectives, leading to confusion and problematic methodology.⁴⁵ The result is an implicit privileging of a point of view, often the external or realist one. This is not surprising. Most legal scholarship has historically been realist.

cyberlaw and emphasizing the importance of recognizing the interconnectedness of both, to preserve the distinctiveness of cyberspaces).

³⁹ Grimmelmann, *Virtual Worlds*, *supra* note 36 (approaching the law within virtual worlds as comparative legal study).

⁴⁰ Zarsky, *supra* note 36 (discussing possible questions raised by virtual worlds for real world laws).

⁴¹ Castronova, *Virtual Economies*, *supra* note 36 (exploring the growth of virtual economies and the impact on real-world economies).

⁴² Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 874 (1996) (arguing that "translation" of constitutional values is the best way to achieve fidelity to the Constitution in cyberspace).

⁴³ See, e.g., Castronova, *Right to Play*, *supra* note 36, at 208-09 (exploring how a "right to play" can be preserved in the face of real world concerns and the hierarchies of "ordinary human affairs"); Grimmelmann, *Virtual Worlds*, *supra* note 36 (exploring software design through lens of virtual world politics); Noveck, *supra* note 36 (discussing questions raised by virtual worlds for real world laws).

⁴⁴ Kerr, *supra* note 14, at 357.

⁴⁵ *Id.* at 357-58 (noting that courts and commentators often switch between external and internal perspective in cyberlaw unknowingly).

Virtualism has recently emerged primarily as a byproduct of the arrival of cyberspace and virtual worlds. Nevertheless, I believe the virtualist perspective is necessary for a sound conceptual and legal understanding of cyberspace and cyberlaw issues.

I hope my ensuing exploration of a virtualist approach to privacy in cyberspace might offer some insight into the ways that perspective can be more than just about *choosing*, but also a way of critiquing approaches to cyberlaw that fail to account for differences between cyberspace and real space. The New Virtualism has important things to say about a number of areas of cyberlaw problems, but to be useful over the long term it must offer sound reasons for advocating a virtualist perspective, demonstrating how it achieves important public policy or legal aims.

III. PRIVACY'S DISCONTENT: CYBERSPACE

A. THE PRESENT SITUATION

We live in a “digital age.”⁴⁶ Politics, society and business deal and trade in information with the assistance of technology. But cyberspace—which I use in this Article as shorthand for the web of private and public “electronics, computers, and communication networks” (most predominantly, the Internet) that “interconnect the world”⁴⁷—offers some of the greatest challenges to privacy.⁴⁸ With its online media and technologies,⁴⁹ computer databases,⁵⁰ and rising tide of digital surveillance,⁵¹ it has long been seen as a threat to privacy in personal information, the “details about our lives we would most often like to keep free from public view.”⁵² Not surprisingly, legal scholars attempting to address privacy concerns in cyberspace have focused on what Paul Schwartz and William Treanor call “the new privacy,” that is, a focus on “informational privacy” and information practices.⁵³

⁴⁶ Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1088, 1091 n.20 (2002) (quoting FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* (1997)).

⁴⁷ Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1195 (1998).

⁴⁸ See Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1610 & n.4 (1999).

⁴⁹ See Kang, *supra* note 47, at 1195.

⁵⁰ See DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 3-4, 13-22 (2004).

⁵¹ See Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297 (2004).

⁵² Sonia K. Katyal, *Privacy vs. Piracy*, 7 YALE J.L. & TECH. 222, 231 (2004); see also Lin, *supra* note 46, at 1091 n.19.

⁵³ Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2164 (2003) (writing that “work inside and outside of the legal academy” has pointed to a “new privacy” focusing on fair information practices, in contrast to “old” or “classic” notions of privacy).

Though defining “informational privacy” is no simple task,⁵⁴ the vast majority of legal scholars have adopted a definition similar to that of the United States Supreme Court in *Whalen v. Roe*⁵⁵—that information privacy concerns a person’s interest in avoiding (and controlling) disclosure of personal matters.⁵⁶ There is no shortage of proposals to achieve such control either in the United States or in other countries, with governments and private industry entering the chorus.⁵⁷ Most legal scholars, influenced by the work of Lawrence Lessig,⁵⁸ have approached the *control* aspect of information privacy as a form of property interest⁵⁹—that is, people ought to be able to control the disclosure and flow of personal information because they have a property interest or right in that information.⁶⁰

Despite these ideas and proposals, privacy is not doing so well these days. In fact, there are deep problems with the present informational privacy paradigm. First, the very notion of “information privacy” causes conceptual problems for our understanding of privacy generally. The concept of privacy, says Daniel Solove, “is . . . in disarray.”⁶¹ It appears to be “about everything, and therefore it appears to be nothing.”⁶² To others, it is a “vague”⁶³ or “chameleon-like”⁶⁴ word that has lived a “vine-like existence.”⁶⁵ After surveying the field

⁵⁴ Lin, *supra* note 46, at 1093 (“Defining informational privacy is a dizzying endeavor . . .”); *see also* Kang, *supra* note 47, at 1202 (“Privacy is a chameleon that shifts meaning depending on context.”).

⁵⁵ 429 U.S. 589 (1977) (deciding a constitutional challenge to a New York statute that required prescriptions for certain drugs to be reported to the state health authorities, leading to the creation of numerous computerized records containing with personal information like the names and addresses of those taking the drugs).

⁵⁶ *Id.* at 598-99; *see also* Kang, *supra* note 47, at 1205; Lin, *supra* note 46, at 1094-95 & n.41; Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000).

⁵⁷ Tal Zarsky, *Desperately Seeking Solutions: Using Implementation Solutions For the Troubles of Information Privacy In the Age Of Data Mining and the Internet Society*, 56 ME. L. REV. 13, 14-15 (2004) (writing of proposals to address information privacy concerns being offer by commercial actors, including the different legal the public policy proposals implemented in other countries and jurisdictions).

⁵⁸ LESSIG, *supra* note 31.

⁵⁹ *See* Lin, *supra* note 46, at 1095 n.44 (citing Schwartz, *supra* note 56, at 820, and Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1446 (2001)).

⁶⁰ *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1287 (2001) (citing Kang, *supra* note 47, at 1246-94).

⁶¹ Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477 (2006).

⁶² *Id.* at 479.

⁶³ ARTHUR R. MILLER, *THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS* 25 (1971).

⁶⁴ Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 458 (1995).

of work on privacy in 1984, Judith Thomas remarked that nobody seemed “to have any very clear idea what [privacy] is.”⁶⁶ Though meant to generate more heat than light, there is certainly some truth to these descriptions of present understandings of privacy.

Unfortunately, the idea of “information privacy” has not helped matters. It simply adds another “category” or “type” to an already complex definition. Today, the concept of privacy is often diced and divided up, factionalized into separate categories.⁶⁷ For example, Jerry Kang divides privacy up into three “clusters” of concern: (a) physical or “spatial” privacy; (b) decisional privacy; and (c) informational privacy.⁶⁸ Anita Allen-Castellitto offers four basic types: physical, decisional, proprietary and informational.⁶⁹ Daniel Solove offers an even broader spectrum of groupings he deems “activities,” such as information collection, information processing, information dissemination, and invasion.⁷⁰ Indeed, getting to know privacy these days is a complicated exercise in taxonomy.⁷¹

Besides rendering conceptualization of privacy more complex and less comprehensible, the present paradigm has other deep problems. First, this model of informational privacy, based on proprietary interest in personal information, offers little certainty in determining privacy claims. In “real space” privacy claims “are often understood as claims against intrusive state action, as a “right held against the state’s power to legislate.”⁷² But in cyberspace, property interests, particularly those represented in copyright, often constitute an equally and potentially greater threat to privacy interests than state action.⁷³ Privacy claims will inevitably clash with property claims in the context of cyberspace. But if privacy is understood mainly in terms of property, there is an impasse in these competing interests.

⁶⁵ Ken Gormley, *One Hundred Years of Privacy*, 154 WIS. L. REV. 1335, 1340 (1992).

⁶⁶ Judith Jarvis Thomas, *The Right to Privacy*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 272 (Ferdinand David Schloeman ed., 1984).

⁶⁷ See, e.g., Anita L. Allen-Castellitto, *The Origins and Growth of U.S. Privacy Law*, 632 PRACTICING L. INST./PATENTS 9, 16 (2001) (dividing privacy up into physical, territorial, decisional, informational).

⁶⁸ See Kang, *supra* note 47, at 1202-03; Lin, *supra* note 46, at 1093.

⁶⁹ See Allen-Castellitto, *supra* note 67, at 16; Lin, *supra* note 46, at 1093.

⁷⁰ Solove, *supra* note 61, at 489.

⁷¹ *Id.* at 485-86.

⁷² Adam Hickey, Note, *Between Two Spheres: Comparing State and Federal Approaches to the Right to Privacy and Prohibitions Against Sodomy*, 111 YALE L.J. 993, 994 n.8 (2002); Jed Rubenfeld, *The Right to Privacy*, 102 HARV. L. REV. 737, 744-50 (1989) (detailing the history of American privacy cases wherein state laws were held to be unconstitutional infringements on certain privacy interests).

⁷³ Katyal, *supra* note 52, at 224 (“[P]roperty rights in cyberspace serve to form the basis for a host of potentially offensive strategies that have deleterious implications for privacy, anonymity, and freedom of expression”).

Take, for example, “piracy surveillance.”⁷⁴ This involves copyright holders conducting surveillance of people’s online activities to detect copyright violations.⁷⁵ People may feel such surveillance is a violation of their privacy, but if they assert their privacy rights in terms of property interest, they will only run up against countervailing property interests in copyright. Here, both privacy and privacy-infringing activities are asserted through property interests, with no apparent calculus or analytical framework to decide between these interests. Julie Cohen has recognized this normative gap. She has argued that the present “property based” approach to informational privacy reduces privacy to little more than individual commodity preferences, such as consumer choices for “black shoes over brown or red wine over white.”⁷⁶ This is a problem because “values of informational privacy are more fundamental” than these sorts of base preferences and choices.⁷⁷ But she also acknowledges that the move from fundamental ideas like human dignity to “fair information practices” is a “leap.”⁷⁸ Why should property interests in information trump other sorts of property interests in copyright? Beyond simply conferring property rights in personal information, a compelling normative rationale must be offered.⁷⁹ The present informational privacy paradigm does not do so.

Moreover, without such a principled rationale to anchor informational privacy to more “fundamental values” (in Cohen’s words), the privacy-as-property model collapses into commodification, increasing the likelihood of privacy-infringing activities. Jessica Litman convincingly argues that the idea of privacy-as-property incentivizes both the collection and transfer of personal information in cyberspace.⁸⁰ Once privacy is understood as an item that is owned as property, commodification slips in, and the free movement of personal information is encouraged. This is easy to see in Platform for Privacy Preferences (P3P), one of Lessig’s suggested solutions to privacy problems in cyberspace.⁸¹ P3P aims to empower user control over

⁷⁴ *Id.* at 228.

⁷⁵ *Id.*

⁷⁶ Julie E. Cohen, *Examined Lives Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423 (2000).

⁷⁷ *Id.*

⁷⁸ *Id.* at 1424.

⁷⁹ Cohen tries to anchor informational privacy to the more “fundamental” ideas of dignity or “informational autonomy,” *id.* at 1423, though it ends up sounding much like the “rhetorics of liberty” she criticizes as glossing over important normative debates. *Id.* at 1423.

⁸⁰ Litman, *supra* note 61, at 1296-98 (arguing that the privacy-as-property model is based on a “fairy tale” assumption that legal ownership of information would enable people to “restrain” their transfer and disclosure). Litman calls Platform for Privacy Preferences (P3P), which Lawrence Lessig has championed for informational privacy protection, the “posterchild” of this flawed assumption.

⁸¹ See LESSIG, *supra* note 31, at 160.

personal data, to allow people to make informed decisions about their personal information.⁸² This is good. But part of this new architecture is the implication that control is for the purpose of data transfer; that personal data can, and perhaps ought to be, bought and sold, leading to the transfer of personal information, the exact activity we ought to be curtailing. If I have a property interest in something, I should be able to sell or exchange it for other preferred goods. Property rights create incentives for alienation and transfer. In fact, when Lessig discusses P3P and similar solutions, he invokes the language of commerce, saying that such code will allow people to properly “negotiate” the terms on which their personal information will be taken.⁸³ Litman’s point is that property interests lead to markets, which only reinforce and promote the transfer and alienation of privacy information from the person. Historically, when people have set out to facilitate the transfer and movement of goods, they have imposed a property rights model.⁸⁴ The privacy-as-property model creates the market for the movement and sale of personal information, thus legitimizing rather than restraining privacy infringement.⁸⁵ I do not think this is inevitable. If there is an intelligible normative framework to anchor privacy interests in cyberspace, which tells us why privacy is important or fundamental, the slide from “property interest” to transfer and commodification may be avoided. But without that anchor, Litman’s concerns are very real. In fact, Lessig recognizes the shortcomings of P3P and the need for “legal regulation” in his updated version of *Code*.⁸⁶

A further important concern involves constitutional protection. There is little hope for the recognition of a constitutional right to “information privacy,” at least on the present conceptual approach. Few commentators believe the U.S. Supreme Court will ever build upon its passing and indirect reference to a type of informational privacy in *Whalen v. Roe*.⁸⁷ As Sonya Katyal has noted, the Court has drawn a “firm line” between “substantive” ideas of privacy relating to issues affecting personhood (like marriage and abortion) and informational ones,⁸⁸ the former having constitutional protection whilst the latter not.⁸⁹ The necessity of constitutional protection remains a contentious issue in privacy scholarship. Early suggestions that

⁸² *See id.*

⁸³ *Id.*

⁸⁴ *See* Litman, *supra* note 60, at 1295-96.

⁸⁵ *See id.* at 1295-96, 1301; *see also* Simon G Davies, *Re-Engineering the Right to Privacy: How Privacy has been Transformed from a Right to a Commodity*, in PHILIP E. AGRE & MARC ROTENBERG, *TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE* 143, 160 (1997) (writing that putting privacy in the “free market environment” creates a situation where privacy “becomes a costly ‘add-on’”).

⁸⁶ LESSIG, *supra* note 7, at 226-27.

⁸⁷ *See* Lin, *supra* note 46, at 1089.

⁸⁸ Katyal, *supra* note 51, at 308; Katyal, *supra* note 52, at 239.

⁸⁹ Katyal, *supra* note 51, at 308; Katyal, *supra* note 52, at 240-41.

constitutional protection was necessary for proper privacy protection⁹⁰ were dismissed by some privacy scholars as unlikely or unnecessary.⁹¹ But as privacy threats continue to grow in cyberspace, the case for constitutional protection has been made more forcefully in recent times.⁹² I do not intend to settle this debate once and for all, but will later offer good reasons why constitutional protection for informational privacy is necessary *and* desirable. Suffice it to say, the present conceptual approach to privacy offers little hope for constitutional recognition in any case.

These problems likely contribute to the most important point—strategies based on the present concept of information privacy do not seem to be working, or, at the very least, have big problems. Today, protection for information privacy in the United States is strewn through a complex web of state and federal laws and regulations.⁹³ Complications with the function of these regulations, the definition and scope of “informational privacy” and the rapidly changing nature of cyberspace and related technology have revealed the “utter inability” of this patchwork of statutes to “keep pace” and “ensure the protection of privacy.”⁹⁴ Particularly, federal statutes in the United States have “faired poorly in cases involving information privacy on the Internet.”⁹⁵ Similarly, solutions to privacy concerns in tort law have been described as “generally useless” in cyberspace,⁹⁶ or in Jessica Litman’s words, involve substantial effort yet ultimately weak protections.⁹⁷

B. THE INTELLECTUAL ORIGINS OF THE PROBLEM: *WHALEN V. ROE* AND THE EXTERNALIST PERSPECTIVE

I believe the intellectual origins of these problems are found in the U.S. Supreme Court decision in *Whalen v. Roe*.⁹⁸ Earlier, I noted

⁹⁰ See David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE W. RES. L. REV. 831, 852 (1991) (arguing for “ultimate protection” for informational privacy through constitutional entrenchment); Francis S. Chlapowski, Note, *The Constitutional Right to Informational Privacy*, 71 B.U. L. REV. 133, 135 (1991) (arguing that informational privacy is a right the Constitution protects).

⁹¹ See, e.g., CATE, *supra* note 46, at 66. Cate concludes that there is little support for informational privacy in the U.S. Constitution.

⁹² See Lin, *supra* note 46; Thomas B. Kearns, Note, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 975, 1003 (1999) (arguing that a “change in constitutional interpretation . . . would align privacy interests and privacy rights”).

⁹³ Katyal, *supra* note 52, at 232 (“Today, informational privacy derives its force from a panoply of federal, state, and regulatory guidelines, many of which emerged from the Code of Fair Information Practices over twenty years ago.”).

⁹⁴ *Id.* at 232-33.

⁹⁵ Lin, *supra* note 46, at 1114.

⁹⁶ *Id.*

⁹⁷ Litman, *supra* note 60, at 1312.

⁹⁸ 429 U.S. 589 (1977).

that the vast majority of legal scholars have adopted a definition for “informational” or “information privacy” similar to that in *Whalen v. Roe*. There, the Court set out to categorize and define different types of privacy interests in the context of the case and, in so doing, created what I believe to be a problematic disconnect between informational and other more established normative foundations for privacy. This needs elaboration.

Privacy in records containing information *about* a person was at issue in *Whalen v. Roe*. The U.S. Supreme Court had to determine the constitutionality of a New York statute that required all prescriptions for a certain class of drugs to be reported to the state Department of Health. The computerized records contained the name, age, and address of drug recipients and were retained for a period of five years for security purposes, to help track unlawful distribution of prescription drugs. A group of patients and physicians challenged the constitutionality of the statute arguing, among other things, that it violated their constitutional right to privacy. In dismissing this argument, the Court distinguished between two separate privacy interests:

The cases sometimes characterized as protecting “privacy” have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.⁹⁹

On the one hand, there is a privacy interest in making important decisions, and on the other, a privacy interest in non-disclosure of personal information. This idea of privacy with its implicit idea of *controlling* personal information in order to prevent unauthorized disclosure is what most privacy scholars have used as the basis for their definitions of “informational privacy.” Though the Court went on to suggest that there may be a constitutional basis for this type of privacy,¹⁰⁰ it has yet to expand on this passing reference and, as noted already, most commentators doubt it ever will.

But let us return to this distinction between a right of non-disclosure and a right in making important decisions. The Court separates these two types of privacy and deals with them individually, finding that the statute was constitutional because it avoided unreasonable disclosure.¹⁰¹ I believe this distinction in *Whalen v. Roe* is a source for some of the conceptual and normative problems for privacy in cyberspace, as it has two subtle but important implications. First, on this reasoning, privacy in personal information ought to be understood as distinct from fundamental decisions a person makes, including intimate decisions about one’s body. Contrary to the Court’s

⁹⁹ *Id.* at 598-99.

¹⁰⁰ *Id.* at 605-06.

¹⁰¹ *Id.* at 601-02.

holding, however, the patients did not view their privacy interest in “avoiding disclosure of personal matters” as distinct from their broader interest in having “independence” to make “important decisions.” The patients saw these as *interrelated*. This is apparent from the flow of their argument, noted by the Court:

Appellees argue that both of these interests are impaired by this statute. The mere existence in readily available form of the information about patients' use of Schedule II drugs creates a genuine concern that the information will become publicly known and that it will adversely affect their reputations. This concern makes some patients reluctant to use, and some doctors reluctant to prescribe, such drugs even when their use is medically indicated. It follows, they argue, that the making of decisions about matters vital to the care of their health is inevitably affected by the statute. Thus, the statute threatens to impair both their interest in the nondisclosure of private information and also their interest in making important decisions independently.¹⁰²

The patients were not just concerned with disclosure, but also the idea that personal information in the hands of others would inhibit their personal decisions about their health, in this case whether to seek drug therapy. Their bid to *prevent* disclosure was inherently tied to their interest in “making important decisions independently,” the decisional component of privacy. As Daniel Solove has noted, the plaintiffs were concerned about their personal information—an “important part of their lives”—being “in the distant hands of the state.”¹⁰³ Concern over this violation of privacy in personal information had a direct impact on the things that the patients felt comfortable doing. In separating out these interests as separate and distinct categories of privacy, the Court disconnected the importance of privacy in information from privacy in decisions, including the *most* private and intimate decisions, those affecting our body and health. Julie Cohen correctly argues that information privacy must be linked to “fundamental” values for more robust privacy protection; yet here, information privacy is disconnected from ideas that relate to fundamental notions of *personhood*, that being the important decisions a person makes.

Second, the Court’s distinction sundered any connection between privacy in personal information and the rich body of constitutional jurisprudence of the Supreme Court that offered *some* foundation for a constitutional right to privacy. As noted by Daniel Solove, the idea of decisional privacy in *Whalen v. Roe* was familiar to the Court’s jurisprudence, being linked to historic privacy cases like *Griswold v. Connecticut*¹⁰⁴ and *Roe v. Wade*.¹⁰⁵ In contrast, the idea of

¹⁰² *Id.* at 598-89.

¹⁰³ SOLOVE, *supra* note 50, at 65.

¹⁰⁴ 381 U.S. 479 (1965) (holding unconstitutional a statute that criminalized contraceptives for married couples because it violated the “zone of privacy”

privacy in non-disclosure “was one that the Court had not previously defined.”¹⁰⁶ By setting privacy in data and information apart from established constitutional privacy jurisprudence, it became very unlikely that a constitutional right to informational privacy would ever be fully developed or articulated in subsequent decisions. In fact, I believe this is a primary reason why the Court so far has failed to do so. In effect, the Court in *Whalen v. Roe* made informational and data privacy a novel constitutional idea standing outside the jurisprudence, rendering it exceedingly more difficult for subsequent courts to build on the idea.

The critic might respond here and say: So what? In real space, the distinction between informational and decisional privacy makes sense. At issue in *Whalen v. Roe* were health records. Records are objects that may contain personal information, but they are clearly distinct from the person and the decisions she makes. In real space the person, with all her interests, rights, and values, *is* disconnected from such objects and the information they might contain, and it would be silly to confuse the two. In a sense, *Whalen v. Roe* incorporates an *externalist* perspective in its approach to informational privacy, discussed earlier. An externalist perspective ignores cyberspaces and virtual worlds and instead conceives the person in real space inputting data and information into electronic or informational outlets, such as a computer, or, in this case, health records. There is nothing wrong with an externalist perspective. It is just one way of approaching the legal and conceptual problems of privacy, and probably worked best on the facts of *Whalen v. Roe*, which involved privacy concerns in real space, and not cyberspace.

But privacy scholars have taken the definition of informational privacy in *Whalen v. Roe* and transplanted it into the context of cyberspace without acknowledging its implicit use of the externalist perspective. Again, this is not surprising. Legal commentators have often overlooked the perspective from which they are approaching legal and factual issues of cyberspace.¹⁰⁷ But in doing so here, they gloss over a number of important questions that, if answered, might offer a more robust concept of privacy, and how it should be understood in virtual worlds and spaces. For example, the distinction between informational and decisional privacy blurs in the context of cyberspace. Information that a person provides in cyberspace inevitably and immediately impacts the course of their journey through cyberspace, including the choices and options available for their browsing or exploration. As Mark Stefik writes, code “determines which people can access which digital objects,”¹⁰⁸ but such regulation

apparent in the penumbras of various constitutional provisions and amendments).

¹⁰⁵ 410 U.S. 113 (1973) (holding that a women’s decision to have an abortion is protected by a constitutional right to privacy).

¹⁰⁶ SOLOVE, *supra* note 50, at 65.

¹⁰⁷ See Kerr, *supra* note 14, at 357-58.

¹⁰⁸ MARK STEFIK, THE INTERNET EDGE: SOCIAL, TECHNICAL, AND LEGAL CHALLENGES FOR A NETWORKED WORLD 14 (1999).

can only be done through what Lessig calls “architectures of control,” technologies of identification that use information *about* a user in cyberspace to govern what they can see and do in cyberspace.¹⁰⁹ Unlike real space where architecture is often difficult to change (fencing, building, land development, security systems, etc. all have significant costs), in cyberspace architecture is determined by code which can, and does, shift dramatically in response to user input. Informational and decisional privacy are inherently linked in cyberspace, and cannot be easily distinguished.

This brief point incorporates a *virtualist* perspective. That is, if we think about a person not as sitting at their keyboard external to virtual spaces (externalist view), but rather choosing, moving, and negotiating *within* virtual spaces (virtualist view), we can see more clearly how the distinction between information and decisionmaking blurs in cyberspace. This is the important analytical difference that a virtualist approach can offer. In fact, I believe many problems with privacy in cyberspace previously outlined can be resolved by discarding the externalism in *Whalen v. Roe* for a *virtualist* account of privacy, which will not only simplify our concept of privacy in cyberspace but reconnect it to stronger normative justifications and constitutional foundations. But what exactly is a “virtualist” take on privacy? And how can it resolve the normative and conceptual problems with privacy apparent in the literature? In the next Part, I take the first steps in answering these questions in setting out what I call a virtualist account of privacy.

IV. A VIRTUALIST ACCOUNT OF PRIVACY IN CYBERSPACE

The problems discussed in the last Part have led some to abandon the project of understanding the concept of privacy altogether. Daniel Solove has recently endeavored to “shift focus away from the vague term” privacy, and instead focus on a project of cataloguing the various specific activities that might be said to impinge upon privacy.¹¹⁰ In this Article I also hope to shift the debate about privacy in cyberspace, but not for the same reasons as Solove. Despite all the problems legal scholars and philosophers have in figuring out how to define privacy, average citizens seem to have a pretty good idea what it is, and how information technology might pose problems for privacy interests.¹¹¹ So while Julie Innis might say that philosophical discussions on privacy are in “chaos,”¹¹² common understanding of privacy is not a lost cause.

¹⁰⁹ LESSIG, *supra* note 7, at 38, 43-54.

¹¹⁰ Solove, *supra* note 61, at 481-83.

¹¹¹ For example, a 2001 survey by the Federal Trade Commission indicated 92% of Americans were “concerned about threats to personal privacy when they use the Internet” and 22% were “very concerned.” See *Federal Trade Commission Materials*, 1241 PRACTICING L. INST./CORP. 731, 762 (2001).

¹¹² JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 3 (1992).

If the concept of privacy is “in disarray,”¹¹³ particularly with respect to cyberspace, it is not necessarily because we do not understand the idea; privacy is, after all, a concept that has been around since ancient times.¹¹⁴ Rather, it is because scholars have not spent enough time theorizing persons and *personhood* in cyberspace. That is, privacy theorists have focused so heavily on defining the right to privacy that they have neglected the right holder, and how we ought to understand him or her *within* the space we call “cyberspace.” This is where a virtualist perspective can offer insight, and a different way of thinking about cyberlaw issues, like privacy. The virtualist perspective takes an “internal” point of view. That means approaching cyberlaw problems from the perspective of a person *internal* to the virtual world or reality created in the “world of cyberspace.”¹¹⁵ The virtualist theorizes the person as someone inhabiting virtual worlds, not in physical but digital form, and choosing, communicating, and traversing the terrain of cyberspace and virtual worlds. In other words, a virtualist account involves an analysis of personhood, and how it ought to be understood in cyberspace.

But before elaborating this account, it is worthwhile to note precisely *why* addressing the question of personhood matters to privacy protection in cyberspace. Personhood provides a conceptual and normative framework for privacy—the idea being that privacy protects the “integrity of the personality” or person.¹¹⁶ Many traditional notions of, and justifications for, privacy are linked to concepts of personhood. Paul Freund, after an exhaustive survey of case law and literature in 1975, related privacy to “personhood,” which he said referred to “those attributes of an individual which are irreducible in his selfhood.”¹¹⁷ Brandeis and Warren famously based their idea of privacy on the similar idea of “inviolable personality.”¹¹⁸ Scholars like Edward Bloustein¹¹⁹ and Jeffrey Reiman,¹²⁰ and philosophers like Stanley Benn,¹²¹ have all offered theories of privacy centered on ideas of

¹¹³ Solove, *supra* note 61, at 477.

¹¹⁴ See RICHARD HIXSON, *PRIVACY IN A PUBLIC SOCIETY: HUMAN RIGHTS IN CONFLICT* 3 (1987); BARRINGTON MOORE, *PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY* 123 (1984) (discussing privacy in ancient Greece).

¹¹⁵ Kerr, *supra* note 14, at 357.

¹¹⁶ Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1116 (2002).

¹¹⁷ J. Braxton Craven, Jr., *Personhood: The Right to be Left Alone*, 1976 DUKE L.J. 699, 702 n.15 (citing Paul Freund, AMERICAN LAW INSTITUTE, 52ND ANNUAL MEETING 42-43 (1975)).

¹¹⁸ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205, 207 (1890).

¹¹⁹ Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 971 (1964) (arguing that privacy protects against conduct that is “demeaning to individuality”).

¹²⁰ Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26, 39 (1976) (asserting that privacy is “essential” to a “complex social practice” of recognition that is a “precondition to personhood”).

¹²¹ Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, NOMOS XII:

personhood. Jed Rubenfeld thus described personhood as the “reigning explanatory concept” on privacy¹²² and today, privacy scholars still focus on it.¹²³ Privacy to a large degree coalesces around the idea of personhood; so if we wish to think about privacy in cyberspace, we should first think about personhood.

A. PERSONHOOD IN CYBERSPACE

Personhood speaks to those very basic things that make us people—in Paul Freund’s terms, the irreducible “attributes of an individual.”¹²⁴ Personhood thus relates to things like “individuality, autonomy, and dignity.”¹²⁵ Part of being an individual is expressing our own unique desires, dreams, goals, and opinions. We make important personal choices and expect others, particularly family and friends, to respect those choices and our responsibility to make them. Respecting personhood means respecting these things, as taking them away, or disrespecting them, would be an affront to our dignity. Classical theories of privacy set out to protect people and to guarantee that respect. Privacy can and should do the same thing in cyberspace.

Central to contemporary theories of privacy and personhood is the idea of self-creation and personal development. Privacy is a “social practice” or ritual that creates the necessary space for personal experimentation and choice, creativity, self-examination, open communication, and dialogue with significant others—those things necessary to allow a person to “shape” his or her “destiny.”¹²⁶ Privacy not only facilitates development of the self, but preserves such development by protecting and respecting the integrity and dignity of the person.¹²⁷ Since personal development and coming to personhood is an ongoing process throughout our lives, privacy is essential to personhood because it creates the conditions necessary for its continuing development and preservation.¹²⁸ Privacy is a precondition to personhood.

These ideas focusing on the individual and personal choices and self-development are linked, at least in part, to traditional theories of the person and personhood. A Kantian theory understands the

PRIVACY 26, 26 (J. Ronald Pennock & J.W. Chapman eds., 1971) (explaining privacy as respect for someone as a person, and his or her interest in personal development).

¹²² Rubenfeld, *supra* note 72, at 739 (1989).

¹²³ See, e.g., Solove, *supra* note 116, at 1116-19 (discussing personhood theories of privacy).

¹²⁴ Craven, *supra* note 117.

¹²⁵ Solove, *supra* note 116, at 1116.

¹²⁶ See Benn, *supra* note 121, at 26; Reiman, *supra* note 121, at 39; Solove, *supra* note 116, at 1116.

¹²⁷ See Reiman, *supra* note 120, at 39; Solove, *supra* note 116, at 1116-17.

¹²⁸ See Reiman, *supra* note 120, at 39-40.

person as a free individual, a rational agent that is an end in itself.¹²⁹ The Kantian person is an abstract one, a conscious, rational, self-determining individual, with preferences and desires. Locke's idea of the person was also abstract, but conceptually distinct from the Kantian view. Locke understood the person as:

a thinking intelligent being, that has reason and reflection, and can consider itself as itself, the same thinking thing, in different times and places; which it does only by that consciousness which is inseparable from thinking, and, as it seems to me, essential to it: it being impossible for any one to perceive without perceiving that he does perceive.¹³⁰

Both Kant and Locke theorized people as contemplative beings, choosing, thinking, and doing. But where Kant emphasized rationality, Locke also believed *continuing* consciousness and memory were essential attributes of the person.¹³¹ Rational choice is only part of it. Those choices also shape our selves and identities over time. Consciousness and memory are the link between choice and self-growth.

But as Margaret Jane Radin notes, both of these “classical views” approach persons as “disembodied minds or immaterial essences.”¹³² Theorists in modern times have thus criticized these classical views as neglecting the importance of *embodiment*, and bodily continuity.¹³³ People are more than just floating disembodied minds; we experience the world and are recognized within and through our bodies. The body, or the idea of embodiment and personhood, is important to privacy. Scholars have argued that one of the key origins of privacy is in property rights,¹³⁴ particularly Lockean theories of property. But that link in many ways was a product of Locke ascribing importance to the body, and our intimate control over our bodies or persons. In the *Second Treatise of Civil Government*, Locke connected property to the person, noting that “every man has a property in his own person: this no body has any right to but himself.”¹³⁵ In a sense, the body, and our intimate control over it, was the foundation of

¹²⁹ DAVID A. J. RICHARDS, *TOLERATION AND THE CONSTITUTION* 78-79 (1986).

¹³⁰ JOHN LOCKE, *AN ESSAY CONCERNING HUMAN UNDERSTANDING* bk. II, ch. XXVII, § 9 (1690), available at <http://etext.library.adelaide.edu.au/locke/john/181u/complete.html>.

¹³¹ Margaret Jane Radin, *Property and Personhood*, 34 *STAN. L. REV.* 957, 963 (1982) (discussing Kantian and Lockean theories of the person).

¹³² *Id.*

¹³³ See, e.g., BARBARA BROOK, *FEMINIST PERSPECTIVES ON THE BODY* 1 (1999) (“What about the body . . . ?”); see also DAVID BELL, *AN INTRODUCTION TO CYBERCULTURES* 138-39 (2002); Radin, *supra* note 131.

¹³⁴ Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 *BERKELEY TECH. L.J.* 1, 26 (1996).

¹³⁵ JOHN LOCKE, *SECOND TREATISE OF CIVIL GOVERNMENT* § 27 (1690), available at <http://etext.library.adelaide.edu.au/locke/john/181s/>.

Locke's theory of property, which understood labor as the basis for property rights in "the earth," which is originally "common to all men."¹³⁶

In contrast to these classical theories, contemporary theories of personhood recognize the importance of the body. If the integrity and dignity of the person is a central normative focus, then privacy in the body and its control, preservation, and inviolability is essential. But this involves more than a Lockean notion of a property interest in the body. It is, as Reiman points out, much more fundamental:

The right to privacy is the right to the existence of a social practice which makes it possible for me to think of this existence as *mine*. This means that it is the right to conditions necessary for me to think of myself as the kind of entity for whom it would be meaningful and important to claim personal and property rights. It should also be clear that the ownership of which I am speaking is surely more fundamental than property rights.¹³⁷

Again, if privacy creates the conditions necessary for personhood, by protecting and preserving the "attributes of an individual which are irreducible,"¹³⁸ then it is prior to any idea of property right or interest.

Is cyberspace any different? What are the "irreducible attributes" of the person in cyberspace that privacy must protect? When I assume an online identity or persona, I am in a Kantian sense still a rational agent and, following Locke, retain a continuing memory and consciousness, not only of my life and identity in real space, but of my activities in cyberspace. So traditional theories of the person certainly still apply, but in focusing solely on attributes of consciousness or theory of mind, they are unable to speak to the differential character of traversing and experiencing virtual worlds and cyberspaces. Moreover, as noted above, critics maintained that traditional theories of the person ignored the physical aspects of being: the limits and boundaries of the body and how we as people interact with the environment. These questions must be explored in relation to cyberspace, too, if personhood is to be properly understood.

So personhood in cyberspace concerns not only real space issues but understanding "the person" in virtual space. In real space the person, and his or her body, is more easily discerned and defined through physical bodily limits and fixed architecture. But in cyberspaces, with their differing electronic environments and shifting digital architecture, platforms, code, identities, and technological capacity, things are a little more complicated. So rather than a unified subject, there are multiple forms of the virtual person in cyberspace.¹³⁹

¹³⁶ *Id.*

¹³⁷ Reiman, *supra* note 120, at 43.

¹³⁸ Craven, *supra* note 117.

¹³⁹ Maria Lugones notably claimed that she was "giving up the claim that the subject is unified." Instead, she would approach "each person" as "many." Virtual

I will discuss three virtualist¹⁴⁰ accounts of the person here: (1) the virtual person in complete virtual reality environments; (2) the virtual person in 3D virtual worlds; and (3) the virtual person as embodied information on the Internet. The latter two notions of personhood in cyberspace are likely most relevant to legal and constitutional protection of privacy, being the ones most people will experience when negotiating cyberspace, but there are likely others.¹⁴¹ This discussion should, in any case, offer a clearer picture of what constitutes personhood in cyberspace, the “irreducible attributes” of the virtual person.

1. The Virtual Person in Complete Virtual Reality Environments

The idea of people existing as entities within virtual spaces or “virtual reality” as an alternative to real space has been popular in modern science fiction. William Gibson is credited with coining the term “cyberspace” in his 1984 novel *Neuromancer*.¹⁴² Gibson famously described cyberspace as a “consensual hallucination” and wrote about the “bodiless exultation of cyberspace” where people “jack in” and leave the “meat” of the physical body.¹⁴³ Such ideas about the synthesis of technology and flesh, virtual reality, and the possibilities of complete virtualized living environments have inspired a whole genre of cultural studies some have called “cyber-cultural theory,” which analyzes the nature of virtual spaces and human behavior within it.¹⁴⁴ As Anne Balsamo notes, virtual reality has become an “industry in itself.”¹⁴⁵

Virtual reality technologies create three dimensional environments into which a person can “enter” and fully interact.¹⁴⁶ The

personhood fits well with Lugones’s theory of personal identity in this way. See Maria Lugones, *Structure/Antistructure and Agency Under Oppression*, 87 J. PHIL. 500, 503 (1990).

¹⁴⁰ These accounts are “virtualist” in that they approach the person and body from the perspective of being internal to cyberspace or the virtual environment.

¹⁴¹ Given the ongoing development of virtual and digital technologies, it would be impossible to conceive of all possible forms of the “personhood” in cyberspace now and in the future.

¹⁴² WILLAM GIBSON, *NEUROMANCER* (1984).

¹⁴³ *Id.* at 12, 67.

¹⁴⁴ See, e.g., ANN BALSAMO, *TECHNOLOGIES OF THE GENDERED BODY: READING CYBORG WOMEN* (1996); DAVID BELL, *AN INTRODUCTION TO CYBERCULTURES* (2002); *THE CYBERCULTURES READER* (David Bell & Barbara Kennedy eds., 2002); *CYBERSPACE/CYBERBODIES/CYBERPUNK: CULTURES OF TECHNOLOGICAL EMBODIMENT* (Michael Featherstone & Robert Burrows eds., 1995); *THE CYBORG HANDBOOK* (Chris Grey ed., 1995); MARK DERY, *ESCAPE VELOCITY: CYBERCULTURE AT THE END OF THE CENTURY* (1996); MARTIN DODGE & ROB KITCHIN, *MAPPING CYBERSPACE* (2000); Donna Haraway, *Cyborgs and Symbionts: Living Together in the New World Order*, in *THE CYBORG HANDBOOK* 11, *supra*.

¹⁴⁵ Anne Balsamo, *The Virtual Body in Cyberspace*, in *THE CYBERCULTURES READER*, *supra* note 144, at 489.

¹⁴⁶ *Id.* at 490.

“cyberspace” here is, literally, the virtual space that a person finds themselves experiencing and moving within the virtual environment. The goal of producing complete virtual environments was originally linked to military research, as well as initiatives in the entertainment industry.¹⁴⁷ Often, this notion of virtual reality, what Balsamo calls its “celebrated media form,” envisions special forms of technology for complete bodily submersion.¹⁴⁸ Thus, the experience requires virtual reality “headsets” and “data gloves” and other innovations necessary for a person to fully escape the limits of real space and the physical body.¹⁴⁹

Complete virtual reality environments are usually promoted as means of freeing oneself from the constraints of real space and the physical body.¹⁵⁰ The person is freed from the body. But this betrays the importance of personhood and the body to virtual reality environments. In actuality, virtual reality technology relies heavily on the physical body and aims to respond to typical body movements, sensations and expression that we usually experience in day to day life. Virtual reality technology attempts to translate information received from the body (and its movements) into a virtualized environment where that information is used to *constitute* your experience. You receive information about the virtual world with which you interact through your senses (via the virtual reality technology), and the technology must receive and process those responses and interactions within the simulated environment to create the virtual reality experience. Information transfer and processing is two way.

The ideal virtual reality technology would offer a seamless interaction between our body in real space and the virtual environment being experienced. But that technology has not yet arrived. The amount of information processing power necessary for such seamless interaction has not been developed and might never be. But before moving on, two points should be stressed. First, information and data plays a key role in this concept of the virtual person. Our 3D persona in the virtual reality environment is created, manipulated, and thus constituted by data provided by our bodies and processed by the virtual reality technology. The virtual person is constituted by information and data *about* us, and our body. Second, the notion of a virtual body is not denied here either. There may be things about our bodies we can change in the complete virtual environment, and we may experience simulated events not usual for everyday life in real space, but this does not mean the body or person is irrelevant; it just means it is less static than usually thought.

¹⁴⁷ See BELL, *supra* note 144, at 140 (talking about “leaving the body” behind as a “recurrent theme in cyberculture”).

¹⁴⁸ Balsamo, *supra* note 145, at 492-93; BELL, *supra* note 144, at 140.

¹⁴⁹ BELL, *supra* note 144, at 14-16 (writing of “VR stories” of virtual reality technology).

¹⁵⁰ See Balsamo, *supra* note 145, at 493 (writing of VR in its “celebrated media form”).

2. The Virtual Person As Avatar in 3D Virtual Worlds

Full-fledged virtual reality technology is not necessary for ideas of persons or personhood in virtual spaces. The rise of virtual worlds and associated innovations like virtual property and commerce offers a similar conceptual understanding of persons in cyberspace, without science-fiction tools or advanced technology. These virtual worlds have emerged in the form of electronic communities¹⁵¹ or complex online multiplayer games (also known as Massive Multiple Online Role Playing Games or MMOGs).¹⁵² These virtual worlds and communities do not require technology for full body submersion within the virtual experience; instead, a user can create a fully three-dimensional person (and radically new virtual bodily and personal identity) in the 3D virtual world, through which he can live, work, and play. A good example of this is the popular online community Second Life. Second Life is a “3-D virtual world” that is “built and owned” by members of the Second Life world. The community offers the complete “architecture of modern societies” with “clothing, buildings, vehicles, and opportunities for starting online businesses.”¹⁵³ According to Second Life’s website, as of mid-2007 there were nearly 7 million members of the virtual community from “around the globe.”¹⁵⁴

Second Life users negotiate the three dimensional virtual space in the community with a user avatar, which is a visible representation of their persona in the virtual world.¹⁵⁵ 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. In fact, Second Life goes far in offering a kind of virtual living—community members can build homes, create art, have relationships with other members of the Second Life world, and make money by trading, buying, and selling their personal virtual items. Indeed, virtual property and virtual commerce in Second Life have grown considerably since 2003, with millions of user-to-user transactions of user-created or owned content and items taking place every year.¹⁵⁶

¹⁵¹ Viktor Mayer-Schönberger & John Crowley, *Napster’s Second Life? The Regulatory Challenge of Virtual Worlds*, 100 Nw. U. L. REV. 1775, 1779 (2006) (referring to Lineage, EverQuest, and Second Life).

¹⁵² See, e.g., Grimmelman, *Virtual Worlds*, *supra* note 36, at 147 n.1 (referring to virtual worlds in large multiplayer online games); Mayer-Schönberger & Crowley, *supra* note 152, at 1781-83.

¹⁵³ Mayer-Schönberger & Crowley, *supra* note 151, at 1787.

¹⁵⁴ Second Life, *What is Second Life?*, <http://secondlife.com/whatis/> (last visited Mar. 29, 2008).

¹⁵⁵ Second Life, *Create an Avatar*, <http://secondlife.com/whatis/avatar.php> (last visited Mar. 29, 2008).

¹⁵⁶ Mayer-Schönberger & Crowley, *supra* note 151, at 1787 (citing Cory Ondrejka, *Escaping the Gilded Cage: User Created Content and Building the Metaverse*, 49 N.Y.L. SCH. L. REV. 81, 93-94 (2004)).

The virtual person, or avatar, in the 3D virtual world is essentially a culmination of data and information—data provided by the person to define and shape their 3D avatar and information relating to the present and past activities of the avatar. This is often called user or “player data.”¹⁵⁷ Player data can include information entered as part of the avatar’s profile as well as the virtual activities of the avatar, such as the different times the avatar engages in certain virtual activities, the types of virtual items bought, places visited, and other virtual persons, or avatars, the virtual person has contacted.¹⁵⁸

Player data is also categorized. It is often defined as either involving identifiable personal information (IPI) or non-identifiable personal information (non-IPI).¹⁵⁹ IPI is information relating to the actual person (in real space) behind the avatar. It can include information about personal characteristics such as culture, age, religion and social status, employment, or credit history, as well as personal contact information like name, mailing address, telephone number, or email.¹⁶⁰ Non-IPI usually concerns “in-world” information. That is, information *about* online or virtual activities *within* cyberspace or virtual worlds that do not link the online persona to the person’s actual identity in real space. Non-IPI involves information gathered from web browsing activities across websites, or from data provided to, or by, third parties.¹⁶¹ In virtual communities, it can include, as noted above, player data relating to virtual activities and virtual commerce with no connection to IPI.

Privacy policies often treat IPI and non-IPI differently. Generally speaking, IPI receives a greater measure of privacy protection than non-IPI.¹⁶² For example, Linden Lab (creators of Second Life) explicitly forbids the disclosure of IPI in its “Community Standards”:

Disclosure

Residents are entitled to a reasonable level of privacy with regard to their Second Lives. Sharing personal information about a fellow Resident – including gender,

¹⁵⁷ Zarsky, *supra* note 36, at 248 (including in player data “data pertaining to the times of the day the player engages in play in general and specific virtual activities in particular, the parts of the virtual world the user visits and the goods she buys, exchanges, and consumes, the other avatars he or she chooses to interact with and the times they do so”).

¹⁵⁸ *Id.*

¹⁵⁹ *Id.* at 249.

¹⁶⁰ Network Advertising Initiative, *Frequently Asked Questions* Nos. 3, 4, <http://www.networkadvertising.org/managing/faqs.asp> (last visited Mar. 29, 2008).

¹⁶¹ *Id.* at No. 4 (“Non-Personally Identifiable Information (Non-IPI) is information that is anonymous or not linked to a particular person. Used for OPM by network advertisers, this data consists mostly of click-stream information (sites you have visited or links you have clicked) compiled as you move across different Web sites or a single site . . .”).

¹⁶² Zarsky, *supra* note 36, at 249.

religion, age, marital status, race, sexual preference, and real-world location beyond what is provided by the Resident in the First Life page of their Resident profile is a violation of that Resident's privacy. Remotely monitoring conversations, posting conversation logs, or sharing conversation logs without consent are all prohibited in Second Life and on the Second Life Forums.¹⁶³

So there is an expectation of privacy between Second Life users with respect to IPI. Linden Lab also sets out in its Privacy Policy that it does not disclose personal information to third parties without permission of the user (with a few enumerated exceptions).¹⁶⁴ But they do not clearly indicate that non-personal information is protected from disclosure, such as the "other pieces of data" mentioned in section 2 of the Privacy Policy, said to be gathered from web traffic, user computer hardware, or Second Life usage. Interestingly, player data can also be public or private within the virtual world. There will invariably be areas in virtual communities inhabited by other members where disclosure of certain information will mean that information is no longer private. Such disclosure is done through display on the avatar profile, user chat, or other forms of virtual activities. Thus, much like the traditional understanding of public and private information, personal information disclosed to other Second Life users, or in "public areas" in the Second Life virtual world, will no longer be treated by Linden Lab as confidential.¹⁶⁵ Player data is thus central to the virtual person in the 3D virtual world. And it is a product of information provided by the creator of the avatar, but also the avatar's activities in his or her virtual community.

In the cyberspace of either the completely virtual environment of virtual reality technology, or the 3D virtual communities of Second Life or EverQuest, conceiving of personhood in cyberspace is quite easy: We visualize the body in space the same way we understand our body in real space. The avatar acts as we do in real space, moving, living, forming relations. Our life choices and preferences are expressed through our avatar, and we respond and relate to others through that same avatar, just as we do in real space. These virtual worlds offer new spaces and social communities to explore while expanding or transforming our individual identity.¹⁶⁶ A lot of cyber-cultural literature focuses on this very idea—how cyberspace and

¹⁶³ Second Life, *Community Standards*, <http://secondlife.com/corporate/cs.php> (last visited Mar. 29, 2008).

¹⁶⁴ Second Life, *Privacy Policy*, <http://secondlife.com/corporate/privacy.php> (last visited Mar. 29, 2008).

¹⁶⁵ *Id.*

¹⁶⁶ See Sherry Turkle, *Our Split Screens*, in *COMMUNITY IN THE DIGITAL AGE: PHILOSOPHY AND PRACTICE* 101, 108 (Andrew Feenberg & Darin Barney eds., 2004) ("[R]elatively consequence-free experimentation facilitates the development of a 'core self,' a personal sense of what gives life meaning . . ."); Zarsky, *supra* note 36, at 251.

virtual worlds liberate the person from his or her real-space identity, and allow creative self-invention and transformation.¹⁶⁷ Moreover, this experimentation can foster better community cohesion and belonging by fostering tolerance and diversity.¹⁶⁸ For many regulars of virtual worlds and communities, their virtual personas can be more significant to their identities than their lives in real space.¹⁶⁹

But this separate virtual identity expressed through the virtual person is maintained with a strong divide, if not barrier, between our physical life in real space, and our online virtual person. A person would not feel comfortable doing certain virtual activities, or engaging with certain people in virtual worlds, if those activities could be linked back to their identity in real space. This is the liberation afforded by anonymity in cyberspace, a shelter for unconventional speech, belief, association, personal preference, and experimentation otherwise suppressed by unpopularity or difference.¹⁷⁰ People often become involved in virtual worlds and communities because they offer a different community to inhabit, learn, and grow. But this sense of belonging and community is threatened where virtual activities, both unconventional and benign, are subject to public exposure or knowledge through linkage to their daily lives in real space. Reputations in real space can be affected by activities in cyberspace.

Reputation can work the other way too. Tal Zarksky makes this point in his discussion of “virtual reputations.”¹⁷¹ Regulars of virtual gaming or virtual worlds can spend years constructing and shaping alternative identities and reputations.¹⁷² Those virtual reputations can be detrimentally affected by information about the person’s actual life in real space. Personally identifiable categories like race, gender, class, and sexual orientation are not necessarily fixed in virtual space. People can experiment and cross these social boundaries. But those experiments are threatened, or can be obliterated, by information about someone’s life or identity in real space. Given the cultural importance of the aforementioned categories, it is not hard to see how someone

¹⁶⁷ See, e.g., BELL, *supra* note 44, 6-29; LISA NAKAMURA, CYBERCULTURE TYPES: RACE, ETHNICITY, AND IDENTITY ON THE INTERNET (2002); Turkle, *supra* note 166.

¹⁶⁸ See SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET 261-62 (1995) (experimentation of multiple selves facilitates understanding of diversity, in contrast to the norm of the “unitary and solid self”).

¹⁶⁹ See Lastowka & Hunter, *Virtual World*, *supra* note 36, at 52 n.280 (describing the growing numbers of people who inhabit virtual worlds and the importance of these virtual communities to their lives).

¹⁷⁰ See Cohen, *supra* note 76, at 1425.

¹⁷¹ See Zarksky, *supra* note 36, at 246 (discussing the case reported in Jim Schaefer, *Sex and the Simulated City: Virtual World Raises Issues in the Real One*, DETROIT FREE PRESS, Jan. 27, 2004). As Zarksky describes it, in this case the identity of one player was revealed by another to be a teenage boy. The disclosure had a serious impact on the “reputation” of the player, as he had been carrying on the virtual persona of a female prostitute. After the disclosure, the player was “obviously” treated much differently by other members of the virtual community.

¹⁷² *Id.*

posing as a virtual person from a different gender or race in Second Life might be treated differently by other users once information about their actual gender or race is disclosed.

Virtual personhood in 3D worlds is, like that of complete virtual reality environments, conceived like our physical persons in real space. We have bodies and we live and engage with others in our community. But the virtual person is, in addition, constituted by information and data. Not only is the very fabric of *being* within virtual worlds constituted by information like player data (such as information provided to create a 3D avatar) but our “virtual” choices, activities, identities, and conduct are also influenced by the flow, exposure, and availability of that information; thus a protective two-way barrier between the virtual person and real person is afforded by the anonymity of cyberspace.

3. The Internet: The Virtual Person as Embodied Information

Unfortunately, the science fiction ideas of William Gibson are not accurate descriptions of most people’s everyday experiences in cyberspace; virtual reality is a developing technology, and certainly not common in households of the average family. Similarly, though online communities like EverQuest and Second Life continue to grow, most people are not members and will not be anytime soon. For most, cyberspace involves negotiating the Internet, and its plethora of discussion boards, websites, file servers, and 2D databases and communities. In these circumstances, without the benefit of a complete three-dimensional world, the externalist perspective seems more natural: People surfing on the web are best understood as real people sitting in front of their computers in real space, rather than any kind of virtual identity or person like that in Second Life.

Still, the virtualist perspective can offer insights here. As Orin Kerr explains, when a person logs onto the Internet and then visits a website like Amazon.com, a virtualist perspective understands the person as visiting a virtual store, looking among the digitized aisles of books and music in much the same way as a customer visits the bookstore in real space.¹⁷³ A Gibson-esque synthesis of technology and flesh is not necessary to understand cyberspace from a virtualist perspective. But what is the virtual person on the Internet? I call it the virtual person as embodied information. Unlike the 3D avatar of Second Life it is more difficult to conceive of virtual persons in the context of simple electronic commerce in virtual stores or wall postings in text-based virtual communities. Yet, this idea is more familiar and intuitive on closer look.

Privacy scholars have already come to identify bits of information and data (particularly those that reveal intimate details about us) that can be collected by tracking a person’s movements on the Internet as constituting a form of virtualized person, or persona. Daniel Solove writes:

¹⁷³ Kerr, *supra* note 14, at 362-63.

Digital technology enables the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own. It is ever more possible to create an electronic collage that covers much of a person's life — a life captured in records, a digital person composed in the collective computer networks of the world.¹⁷⁴

The collection of intimate information about a person, what Solove calls a “digital person” or “digital dossier,”¹⁷⁵ can offer a detailed and complete mapping of the person, a “life captured in records.” Our identities, personal preferences, interests, relationships (online and offline), health, hobbies, and work are embodied in the information volunteered by us online, or collected about us through our daily sojourns in virtual worlds, electronic landscapes and virtual commerce.¹⁷⁶ Similarly, Katyal invokes the “virtual persona,”¹⁷⁷ and Patrica Mell the “electronic persona.”¹⁷⁸ This electronic “compilation of bits of personal information concerning the individual” can perform a number of different functions for varying parties in the digital context, including acting as an invaluable information resource for governmental and commercial entities.¹⁷⁹ Our identity and persona in cyberspace is very much the information *about us*.

Does it make any sense to analogize a profile of data and information to ideas like virtual bodies and persons? In real space it makes little sense, but in cyberspace it does on several levels. First, the idea of the virtual person as embodied information is not inconsistent with traditional theories of personhood that spoke to consciousness and memory. Following Lockean or Kantian theories, when we traverse online communities and worlds our subjective consciousness remains intact; we are as we were before, though we sometimes assume different signifiers of identity (such as using a different username to explore with anonymity). Our memories, consciousness, thoughts, and desires carry over from real space, though they might be expressed differently with the new landscapes and anonymity that cyberspace provides. The difference with this approach to personhood in cyberspace is an emphasis on how the virtual person is constituted by

¹⁷⁴ SOLOVE, *supra* note 50, at 1.

¹⁷⁵ *Id.* at 1-2.

¹⁷⁶ Online search histories collected by Google, Yahoo, and MSN search engines are a good example of this. Take Google, for instance: not only is every search request entered by a user recorded and stored by Google, but the searches are logged to a specific IP address. Every single online search can be linked back to a specific location in cyberspace. This information can be retrieved by Google, and in fact the U.S. government has asked for this information before (though Google refused, Yahoo and MSN did not). See LESSIG, *supra* note 7, at 204.

¹⁷⁷ Katyal, *supra* note 52, at 243.

¹⁷⁸ Mell, *supra* note 134, at 3.

¹⁷⁹ *Id.* at 4.

bits of data and information online, so that from a virtualist perspective we understand the person as an embodiment of that information.

Second, the virtualist perspective requires relinquishing ideas of physical bodies and persons for virtual ones. After all, the divide between the “physical person” and information about the person is hard to maintain in the informational landscapes of cyberspace. The law often draws a clear line between the physical body or the person, and information and records about the person. The former retains strong legal and privacy protections, and the latter much less so. But just as the distinction between decisional and informational privacy is blurred in cyberspace, so too is the distinction between the person and information about the person.¹⁸⁰ A good example of this is computerized medical health information, particularly electronic databases containing complete maps of a person’s genetic code or biometric information which offer an individualized “link” (like DNA fingerprinting) between the record and a specific person.¹⁸¹ Such information often constitutes some of the most intimate details about a person and the life they lead today or tomorrow. Traditional distinctions between physical bodily integrity and information about the body are unable to account for the ways in which intimate details about our physical bodies are being integrated into informational systems and digitized records.¹⁸² You cannot study, understand, or track a person’s genetic code without a material rendering of it, and cannot analyze, store, or quantify it without an information or digital records system. Here, the physical body becomes, in Irma van der Ploeg’s words, the “body as information.”¹⁸³ New conceptual and normative categories of privacy are thus required, as the old categories of bodily integrity (“the person”) and information (“representations of the person”) break down.¹⁸⁴

Additionally, the virtual person as embodied information captures an important aspect of online experience that links autonomy and liberty to informational identity. Privacy scholars like Patricia Mell often decry how personal information collected about people from their activities in cyberspace is used by governments for decisionmaking and by commercial entities for market research.¹⁸⁵ But there is a further dimension to this in how the information we volunteer or is tracked *about us* shapes the places we can go, the things we can

¹⁸⁰ Irma van der Ploeg points out that data protection regimes, such as the European Directive on Data Protection, focus on informational privacy but neglect the ways that the body itself is being integrated within information systems, blurring the lines between (physical) bodily integrity and protection of personal information about the body. Irma van der Ploeg, *Biometrics and the Body*, in *SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK AND DIGITAL DISCRIMINATION* 57, 66-67 (David Lyon ed., 2003).

¹⁸¹ *Id.* at 63-64.

¹⁸² *Id.* at 66-67.

¹⁸³ *See id.* at 64.

¹⁸⁴ *Id.* at 66-67.

¹⁸⁵ Mell, *supra* note 134, at 3.

see, and the choices we make in the cyberspaces we traverse. This information is what we defined earlier as non-IPI. This data is not linked to your actual physical identity, but can still be used to shape, constrain, and alter your travels in cyberspace. As Lessig has taught us, in real space architecture can limit where we can traverse, but many of these barriers are static and unchanging. Thus, a wall or fence prevents us from trespassing in a yard, but the public road remains open for our use regardless of our identity. In cyberspace, architecture is much more fluid, determined primarily by code, software, and hardware limitations.

The architecture of cyberspace can also shift and change in accordance with the specific person doing the traveling and exploring. On a simple level, this is apparent with passwords that restrict access to certain sites online. Only those who have the password can gain access. But there are other more sophisticated forms of verification, such as “cookie” files, tiny files on your hard drive that help sites identify you and your computer on future visits.¹⁸⁶ People often allow cookies to move freely between their computer and the various sites visited online. Cookies offer not only a form of digital verification, but also accumulate and provide information about user preference; cookies can tell a site (like Amazon.com) information about the user, like the types of music they prefer, the movies they have purchased, or online searches previously conducted. This data shapes the choices made available as the user negotiates Amazon.com’s virtual shelves.¹⁸⁷

Other forms of informational identification in cyberspace similarly shape the online experience, like “digital certificates” that reside on your computer and act, in Lessig’s terms, as a form of “passport” to negotiate sites, allowing access in some places and restricting it in others.¹⁸⁸ Again, these things speak to aspects of personhood, our “individuality, dignity, and autonomy.”¹⁸⁹ Information *about us* affects our freedom and autonomy; it shapes the places we can go in cyberspace, the same way our physical bodies limit the places we can go in real space. The virtual person as embodied information recognizes this reality. This is important. For as these “architectures of control” and digital forms of “authentication”¹⁹⁰ develop and advance, this aspect of online experience will only magnify and become of greater concern to those like Lessig, who are concerned about privacy, freedom and liberty in cyberspace.

Consistent with the New Virtualism, the idea of the virtual person as embodied information speaks to our experience within cyberspace, but draws connections to our lives in real space. That is, we are two persons—even two bodies—the one in real space, which is

¹⁸⁶ See LESSIG, *supra* note 7, at 47.

¹⁸⁷ Amazon will recommend books and others things to buy. See LESSIG, *supra* note 30, at 34.

¹⁸⁸ *Id.* at 35.

¹⁸⁹ Solove, *supra* note 116, at 1116.

¹⁹⁰ LESSIG, *supra* note 30, at 30-31.

constituted by our physical bodies (from an external or realist perspective), and the one in cyberspace (from a virtualist perspective), which is constituted by the “body as information.” The “body as information” includes the very basic information that makes our travels in cyberspace possible (such as our physical IP address) and more intimate personal information, such as IPI and data about our lives and health often volunteered by us (sometimes unknowingly) or collected through subtle tracking of our movements and activities online.¹⁹¹ But the virtual person as embodied information also emphasizes the important connections between these two personas; for as van der Ploeg has illustrated, the virtual person implicates many intimate aspects of our physical well-being in real space. The point here is not that intimate information creates an actual physical bodily form in virtual spaces cut off from our selves in real space, but from a virtualist account, this information is central to our identity and personhood in cyberspace.

B. CONCEPTUALIZING VIRTUALIST PRIVACY

The externalist view quietly pervades privacy scholarship on cyberspace.¹⁹² Perhaps for practical reasons, it makes sense for lawyers and judges to think of people in the everyday sense, as people who live, who have jobs and families and common responsibilities, and also, perhaps on a daily basis, communicate through or explore cyberspace. Here, cyberspace simply refers to a lot of wires and hardware: computer stations, file servers, databases, networks, software applications and, of course, code. People do not “enter” cyberspace, they simply use it, sitting at their computer desks or laptops. We are always outside looking in. And so is the law. A virtualist would say this externalist account ignores the unique experience of traversing cyberspace and virtual worlds. We must, as a starting point, investigate the person as present *within* a virtual place in ways different from real or physical space.

I have attempted to explore some of the different dimensions of personhood in cyberspace. This is important, since personhood, to a large extent, provides a conceptual and normative framework for privacy—it protects the “integrity” of the person.¹⁹³ But more questions are raised here. How do we conceptualize privacy with respect to these different ideas about personhood in cyberspace? The primary purpose of my argument here has been to demonstrate the utility of the virtualist perspective and shift the frame of discussion to

¹⁹¹ Katyal, *supra* note 52, at 255 (“Today, techniques of data collection are especially pernicious because they are subtle, ongoing, largely unregulated, and inextricably linked to a person’s online activities. Various entities collect an enormous amount of personal information from users with scant attention to the moral and legal privacy implications raised by its collection.”).

¹⁹² But as Orin Kerr notes, there are some important exceptions, like the work of Lawrence Lessig. See Kerr, *supra* note 14, at 370-371.

¹⁹³ See Solove, *supra* note 116, at 1116 (describing the personhood conception of privacy).

focus less on dividing, categorizing, and dicing up our ideas and concepts of privacy, and think more about the *subject* of privacy being the *person* (or the virtual person); as such, I do not intend to set out an exhaustive account of “virtualist privacy.” I will, however, offer a basic theoretical framework and raise issues for further exploration and research.

1. The Irreducible Attributes of Personhood in Cyberspace

If privacy concerns the inviolability or integrity of persons, it must protect those things essential to personhood. Virtualist privacy thus targets those “irreducible attributes” of the virtual person in cyberspace that relate to “individuality, dignity, and autonomy.”¹⁹⁴ But what are these attributes? Our discussion of three different conceptions of the virtual person in cyberspace offers some insight. First, virtual personhood is constituted by data and information. I mean this not only in the obvious sense that virtual worlds and cyberspaces are products of code and therefore must consist of bits of data, but also in the sense that our virtual identities, activities, and personas are primarily shaped and influenced not only by data we volunteer (such as data to create a 3D avatar) but also information gathered or available about our activities, whether virtual commerce in Second Life or web browsing on the Internet. This shapes not only our autonomy and behavior (and freedom to act as we choose), but also the physical contours of our travels in cyberspace. Architecture in cyberspace is fluid and shaped by a two-way flow of information between the virtual traveler and the destinations.

Second, the integrity of virtual personhood requires real space and virtual space to remain disconnected and distinct. This divide is maintained by the anonymity of cyberspace, which offers shelter to allow people to learn, grow, transform identity, and find a new sense of belonging in a virtual community sometimes radically different from the one negotiated in their actual lives. Disclosure and other means of linking virtual and real lives threaten such exploration, damaging either real world or virtual world identity. Ideas like “virtual reputation[.]”¹⁹⁵ and the importance of membership in virtual communities (to many virtual world citizens), both 3D and on the Internet, illustrate that virtual personhood must occupy a *distinct* place, isolated from real space identities, responsibilities and communities.

Third, virtual personhood involves more than just a “rational mind” or a continuing consciousness negotiating cyberspace in the Kantian and Lockean sense. There is an aspect of embodiment to virtual persons. This is obvious in the case of the virtual person in a complete virtual reality environment or the 3D avatar in a virtual world. Here, there is an actual representation of the virtual body in cyberspace. Yet, as I have argued, there is also an element of embodiment in the 2D environs of the Internet. From a virtualist

¹⁹⁴ *Id.*

¹⁹⁵ Zarsky, *supra* note 36, at 246.

perspective, the digital dossiers or profiles *about* us, and the information and data collected about our activities (like web browsing) that can be linked to our IP address, both intimate and otherwise, embody or “make up” our virtual person in these cyberspaces, governed and shaped by information and data. This data attaches to, and constitutes, our virtual identity.

Once again, virtual persons should not be understood as somehow cut off or disconnected from our actual selves in real space, thus raising independent privacy interests. To the contrary, virtual personhood is an extension or emanation inextricably linked to our actual lives and identities, with real implications for our freedom, intimacy and dignity. Virtualist privacy just offers the best way to address these unique issues.

2. Toward a Theory of Virtualist Privacy

A theory of virtualist privacy should, at its foundation, protect these attributes of virtual personhood. Not surprisingly, these attributes also have implications for the types of legal and theoretical tools necessary to properly protect privacy in cyberspace. Virtualist privacy requires by logical necessity a form of informational privacy. If virtual personhood is constituted by data and information at the most basic and fundamental level, then protecting privacy of virtual persons will require privacy in data and information. An important difference between this reliance on a form of informational privacy and the predominant idea of “information privacy” in privacy scholarship is that the latter is often set out as a new “type” or “category” for the concept of privacy to cover. Traditionally, the concept of privacy covers things related to privacy of the person—autonomy, decisional privacy, protection from government intrusion in our private and intimate lives. Traditional privacy scholarship (probably unwittingly) deploys an externalist perspective and thus must tack on “informational privacy” as a new ground for the traditional concept to cover.

Virtualist privacy avoids these complications. On a virtualist perspective, the virtual person is constituted by information or data, so privacy of the virtual person requires privacy in these constitutive parts. The concept of privacy does not need to be transformed to account for cyberspace; rather, it must simply be applied in its traditional conceptual understanding *within* cyberspace, the realm of virtual persons. Unlike the externalist perspective from real space where informational privacy must be explained as somehow attaching to information records and data, from a virtualist approach privacy attaches to the virtual persona. It just so happens that the virtual person is constituted by data and information in its various permutations and forms: in complete virtual reality environments and virtual worlds, and on the Internet.

So a virtualist approach to privacy in cyberspace requires informational privacy. What sort of conceptual framework is necessary to protect the irreducible attributes of virtual personhood? I recognize that strong privacy protections for *all* of the personal information about

us available online would go too far, and restrict the flow of information. Often, we *want* some information about us to be offered to sites (i.e. bits of data in cookies) to make our online travels more convenient or easier to negotiate. But other more intimate personal information could receive greater protection. There needs to be a practical balance.

A virtualist approach might protect three primary spheres of privacy relating to the virtual person. The first sphere offers strong privacy protections for any personal information that would tend to “link” the virtual person to the actual person in real space. This includes most prominently identifiable personal information (IPI): names, addresses, phone numbers, email, as well as information like race, age, gender, employment, and credit history, which could reveal identity if synthesized with other available personal information. For example, virtualist privacy would advocate strong protection against disclosure of information that would link a person’s IP address, or other digital identifier, to their actual home address or other IPI. Or in another case, player data from a virtual world multiplayer game or virtual community that consists of IPI would be protected from disclosure to other virtual players, to protect identities and reputations.

One way to think about this sphere of virtualist privacy is in terms of more traditional ideas about privacy—protection against disclosure for IPI and other intimate information that reveals identity would protect individuals from humiliation or loss of dignity if certain virtual activities were linked to the person in real space.¹⁹⁶ This is privacy of the individual against unreasonable or unjustified intrusions.¹⁹⁷ Privacy protection is often framed on the basis of dignity (as personhood has long been an important aspect of privacy), but again, the problem with these traditional notions of privacy is that they cannot account for informational privacy.

This sphere of protection also finds some rationale in the many normative justifications for anonymity in cyberspace. These have been convincingly advanced by others like Julie Cohen,¹⁹⁸ and I need not repeat them here. Essentially, this sphere of protection relates to the idea of virtual personhood, as informational links between real-space identity and virtual persons can detrimentally impact reputation and individual identity on both sides of the divide. The “threat” to privacy along these lines is posed both by government and private actors. As Tal Zarksky points out, governments often have the capacity to collect personal information about us in cyberspace *and* link that information to our identities in real space.¹⁹⁹ In some cases, disclosure of IPI can obliterate virtual personas built on self-learning and reinvention. An

¹⁹⁶ See LESSIG, *supra* note 30, at 147-48 (examining the possibility of protection applied to the concept of privacy as dignity).

¹⁹⁷ *Id.*

¹⁹⁸ Julie Cohen, *A Right to Read Anonymously: A Closer Look at “Copyright Management” in Cyberspace*, 28 U. CONN. L. REV. 981 (1991).

¹⁹⁹ Zarksky, *supra* note 36, at 243-44.

informational privacy regime that guaranteed protection from disclosure of information that could easily link our identities would attenuate these threats. This sphere of privacy protection applies to ideas of the virtual person both in 3D virtual worlds and the 2D spaces of the Internet.

The second and third spheres or areas of virtualist privacy would cast the net of informational privacy wider still, focusing on privacy attached to the virtual person, including the virtual body. The focus here shifts to the preservation of the autonomy and decisional liberty of the *virtual person* in cyberspace. The privacy laws and other regulatory schemes normally discussed by privacy theorists offer measures to protect and preserve the privacy and autonomy of the person in real space—privacy protection for home, work, intimate relationships, etc. Virtualist privacy would do the same thing, but instead propose strict privacy practices *in cyberspace*, which focus on and attach to the virtual person and their virtual activities. As already noted, for many people their virtual persona is more central or integral to their sense of self than their physical lives in real space.²⁰⁰ If this is the future direction of virtual life and cyberspace, then it is worthwhile conceiving of people possessing distinct privacy rights and protections both in their real space *and* virtual persons.²⁰¹ This is what the virtualist perspective demands.

The second sphere of virtualist privacy would require stricter privacy practices to protect virtual persons against massive collection and compiling of information about, or attached to, their online or virtual activities (such as compiling of extensive player data). Such privacy protections would help preserve the autonomy and liberty of virtual persons in cyberspace. Information profiling and collection and transmission of massive bits of data on virtual and online activities creates what Sonia Katyal calls a “culture of panopticism” where individuals discipline and normalize their behavior for fear of being watched or monitored.²⁰² This has a subtle but profound impact on conduct, even in the virtual and often anonymous environments of cyberspace. In Daniel Solove’s words: “By constantly living under the reality that one could be observed at any time, people assimilate the effects of surveillance into themselves. They obey not because they are monitored but because of their fear that they could be watched. This fear alone is sufficient to achieve control.”²⁰³ As in real space, people living through virtual persons suppress behavior under the constant threat of data monitoring and collection.

These concerns are also linked to virtualist privacy protection for IPI. With greater amounts of information compiled and attaching to a virtual person (like player data in a virtual world), there is a greater possibility that more intimate information (like IPI) could be mixed

²⁰⁰ See Lastowka & Hunter, *Virtual World*, *supra* note 36, at 52 n.280.

²⁰¹ *But see* Zarsky, *supra* note 36, at 251-52 (asserting that it is too soon to tell).

²⁰² Katyal, *supra* note 51, at 300, 318.

²⁰³ Solove, *supra* note 59, at 1415.

with more benign data, and thus could be disclosed, leading to humiliation or “links” between real space and virtual identity. This second sphere of virtualist privacy would thus require privacy practices to regulate collection of information in virtual worlds, like player data, so as to limit its scope and flow (particularly from private to public hands). There is also a communitarian rationale underlying these measures. Communitarian arguments are usually offered to oppose privacy arguments.²⁰⁴ But my concern here is *virtual communities*. Without these important protections for virtual persons, which allow for self-determination, unconventional expression and other virtual activities, communities in virtual environments will suffer.²⁰⁵

This third sphere of virtualist privacy offers more experimental ideas about privacy in cyberspace. The focus is less on IPI or information and data collection and compiling than on the specific privacy interests of virtual persons living and engaging with others in virtual worlds. Virtual persons have privacy interests in virtual space, just as persons have similar interests in real space. Though novel, I would argue that these ideas follow intuitively from certain conceptions of the virtual person. As already noted, conceiving of personhood in these 3D cyberspaces is easy because our bodies and actions are represented in these virtualized environments in the same way we understand our bodies in real space. The person acts as we do in real space, making choices, moving, living, forming relations. Applying concepts of privacy to these circumstances are natural; the virtual person—represented in a three-dimensional world by an avatar—should receive the same bodily and spatial privacy considerations as our persons in real space. Personal space and personal creations of virtual community members should be shielded from view, subject to the same privacy protections as such intimate areas of creativity and living in real space.

So, for example, one might suggest that a person’s activities in his virtual house in Second Life ought to be protected from the prying eyes of other members of the virtual community and quite possibly legal authorities. Indeed, the extent and application of privacy in virtual worlds is presently a live issue for legal authorities and governments. Just as legal disputes within virtual communities are inevitable,²⁰⁶ so too are disputes about privacy protections for virtual persons in 3D worlds. In April of 2007, it was reported that the Federal Bureau of Investigation was invited by Linden Lab to investigate allegations of (potentially illegal) virtual gambling being conducted in

²⁰⁴ See Cohen, *supra* note 76, at 1428-29 (discussing the argument that restrictions on flow of information could harm community interest in public safety and health, by preventing such information from being disclosed).

²⁰⁵ See *id.* at 1426; see also Thomas C. Anderson, *The Body and Communities in Cyberspace: A Marcellian Analysis*, 2 ETHICS & INFO. TECH. 153, 153-54 (2000) (describing the freedoms of the virtual community).

²⁰⁶ See Phil Davis, *Second Life Spawns Real World Law Suite*, CHARLOTTE SUN-HERALD, Aug. 7, 2007, available at <http://www.sun-herald.com/floridanews.cfm?id=304>.

Second Life's virtual world.²⁰⁷ Such circumstances raise issues of the application of traditional privacy protections from government searches and investigations, but with the complication of this being virtual, not real, space. If illegal virtual activities are, nonetheless, done in the sanctity of a Second Life user's home, should there be special protection against intrusions into that home? Though virtual gambling may violate anti-gambling statutes, lawyers should ask what sort of legal obligations Linden Lab has to its users and what sort of restrictions there should be on government investigations in virtual spaces, given reasonable expectations of privacy against such investigations in comparable real spaces. Of course, these points raise a number of complex regulatory questions concerning the application of laws to virtual worlds that go beyond the scope of this Article. My point, however, is that ideas about privacy are certainly not alien to the 3D virtual worlds of cyberspace.

If privacy protects the "integrity of the personality,"²⁰⁸ or person, then figuring out the "person" in cyberspace is necessary to protecting integrity through privacy. While not offering an exhaustive account, I have attempted to elaborate the "person" in cyberspace and provide a starting framework for discussion about virtualist privacy. Again, questions are raised: Why should privacy theorists even consider the virtualist perspective? What are the benefits? Or is virtualism just a conceptual slight of hand, with no impact on present ideas about privacy and its justification? The next Part sets out to answer these questions and others.

V. WHY VIRTUALIST PRIVACY?

The distinction between external and virtualist perspectives is primarily an analytical tool. It helps us make sense of different theoretical and normative problems concerning law and technology. But it can transform our ways of thinking about these problems too, illustrating new ways to approach older legal problems. I believe this is the case with privacy in cyberspace. Virtualist privacy has three advantages: (a) conceptual and normative; (b) constitutional; and (c) technical/public policy.

A. NORMATIVE AND CONCEPTUAL ADVANTAGE

1. Simplifying the Concept of Privacy

A person negotiating cyberspace makes personal choices, discloses intimate information, and engages in activities she or he would prefer remained private. But as Lessig notes, data and information collection is the "dominant activity of commercial websites," with ninety-two percent collecting, sorting and compiling

²⁰⁷ See Adam Pasick, *FBI Checks Gambling in Second Life Virtual World*, REUTERS, Aug. 4, 2007, available at <http://www.reuters.com/article/technologyNews/idUSHUN43981820070404>.

²⁰⁸ Solove, *supra* note 116, at 1116 (discussing the conception of privacy as related to personhood).

personal data from web users.²⁰⁹ Oscar Gandy calls it the “panoptic sort,” with cyberspace constituting and incorporating a massive structure for the collection of data and, with it, subtle and overt forms of discrimination based on that data.²¹⁰ This data compilation and the privacy threat it poses reduces our liberty and freedom in cyberspace.²¹¹ For example, few people would conduct online searches freely (particularly when searching for controversial material), if each query were being logged to their profile or logfile linked to their internet provider address.

Lack of informational privacy affects our autonomy and decisionmaking in cyberspace in other ways. As discussed earlier, information collected and made available *about us* in cyberspace often plays an important role in setting boundaries on our autonomy, the places we can go, things we can see; cookies, digital certificates and other forms of digital authentication, our physical IP addresses, data we provide to online sites that is then shared with others—these and other bits of information shape our experience and travels in different cyberspaces. We should be concerned about this “profiling” not only because it can be easily linked to our identities in real space, causing humiliation or loss of dignity, but for other reasons, too. As Lessig points out, as the “system” watches, it forces people into patterns that limit options and diversity of choice in cyberspace (it collects data about you, generalizes your preferences, and feeds them back to you, creating a cycle).²¹² This also disrupts the diversity and cohesion of online communities by creating “zones” of economic or personal preference.²¹³

These and other circumstances demonstrate the necessity of privacy, and how traditional concern for autonomy and decisional privacy—ideas linked to privacy and personhood—apply to cyberspace as much as real space. But on present theoretical and conceptual approaches, a new “type” of privacy, informational, is seen as necessary to address these concerns in the new context of cyberspace, adding an already over-stretched and overly categorized concept. Hence, Solove describes the concept of privacy as in

²⁰⁹ LESSIG, *supra* note 7, at 219.

²¹⁰ *Id.* (citing OSCAR GANDY, *THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION* (1993)).

²¹¹ Privacy promotes liberty and freedom by allowing us to engage in “unconventional” and “unpopular” activities. *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 455 (1980) (arguing that “privacy is . . . essential to democratic governance because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy”); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1665 (1999) (arguing that privacy influences “the extent to which certain actions or expressions of identity are encouraged or discouraged”); *see also* Daniel J. Solove, *A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere*, 84 WASH. U. L. REV. 1195, 1199 (2006).

²¹² LESSIG, *supra* note 7, at 220.

²¹³ *Id.*

“disarray,”²¹⁴ something that appears to be about “everything” and therefore about “nothing.”²¹⁵ The emergence of cyberspace means that privacy is now faced with an entirely new and unique context to protect, and in many ways the concept is still running (or being stretched) to catch up with these changes. For this reason, privacy theorists have taken the simple but less imaginative route of enumerating cyberspace—and the informational privacy it requires—as a new “concern” that requires a new “type” of privacy (informational). This means that privacy has been diced and divided up even more. A good example of this is Jerry Kang’s focus on three “clusters” of privacy: physical or spatial, decisional, and informational.²¹⁶

A virtualist approach to privacy in cyberspace avoids these added complications. If persons are conceived as virtual persons *within* cyberspace then privacy can be linked back to other, more familiar notions of privacy centered on personhood. There is no need to posit an additional “type” of privacy relating to information. This is easily seen, for example, with the virtual person in virtual 3D worlds. The virtual person in these contexts is simply a culmination of information—both data entered to create the 3D avatar, and data relating to the present and past activities of the avatar. Similarly, the virtual person as embodied information also links privacy to the person. The “person” is, much like the 3D avatar, a culmination of data and information beginning with the IP address and all bits of data logged and relating to that address, be it online searches, surfing habits, or information disclosed, collected, or dispersed. Some of this information is intimate, some less so, but nonetheless it all constitutes the “virtual person” from a virtualist perspective. In cyberspace we become an informational profile and the information embodies our person. Should not this virtual person, this “digital person” (in Solove’s terms) have similarly strong privacy protections as our persons in real space?

Conferring privacy protections on virtual persons requires by necessity privacy in information; virtual persons are *constituted* by information and data. They are one and the same. Virtualist privacy, in other words, simplifies our concept of privacy. It does not require formulation of a new vocabulary to speak to privacy in digital or virtual contexts. Rather, we theorize persons in cyberspace and contextualize privacy, rather than re-categorizing it endlessly.

2. Justifying Privacy in Data and Information

A central challenge for those hoping to strengthen privacy in information and data—things that constitute *and* shape our experience and activities in cyberspace—is to offer a compelling normative justification for this “new” (or newer) “type” of privacy. This is not

²¹⁴ Solove, *supra* note 61, at 477.

²¹⁵ *Id.* at 479.

²¹⁶ Kang, *supra* note 47, at 1202-03; *see also* Lin, *supra* note 46, at 1093.

only a philosophical, legal, or ethical concern. It is a public policy one, too. Raising public awareness about threats to privacy on the Internet and other electronic networks and promoting what Paul Schwartz calls “privacy norms for information”²¹⁷ are essential to meet the challenges technology and cyberspace pose to the privacy, liberty and autonomy of citizens.²¹⁸ But to get there, a normative justification or foundation for informational privacy is necessary. This passage from Lessig’s *Code 2.0* illustrates this reflexive need:

But (at least some kinds of) information about individuals should be treated differently. . . . Individuals should be able to control information about themselves. We should be eager to help them protect that information by giving them the structures and the rights to do so. We value, or want, our peace. And thus, a regime that allows us such peace by giving us control over private information is a regime consonant with public values. It is a regime that public authorities should support.²¹⁹

Notice Lessig’s language. We “should” protect information. We “value” privacy. Public authorities “should” support a regime that protects informational privacy. But again, this returns to the question—what is the normative and conceptual basis for informational privacy? The predominant approach has been to link informational privacy to property interests. But this has failed for a number of reasons (discussed earlier in Part III), not the least of which is that in cyberspace the technologies that threaten privacy are often themselves advanced with recourse to property rights and interests, reducing privacy to a low-level interest often outweighed by more powerful property interests and stakeholders.²²⁰

Informational and data privacy needs a stronger foundation. Julie Cohen has recognized this. She writes that informational privacy interests are more fundamental than the present property-based regime.²²¹ But she admits the move from fundamental ideas like human dignity to information privacy is a “leap.”²²² On first take, Cohen seems right. How can electronic records, data, and other bits of information be connected to people? But it only seems like a normative gap from an externalist perspective. If people are understood as external from cyberspace and cut off from the information and data that constitutes their persons and identities in these contexts, then yes, connecting those external and remote bits of information to more

²¹⁷ Schwartz, *supra* note 56, at 858.

²¹⁸ *See id.* at 858-60.

²¹⁹ LESSIG, *supra* note 7, at 231.

²²⁰ *See my discussion of piracy surveillance, supra* Part III.

²²¹ Cohen, *supra* note 76, at 1423.

²²² *Id.* at 1424.

fundamental ideas like human dignity and privacy of the person requires a great normative leap.

A virtualist approach to privacy in cyberspace avoids this normative gap. From an externalist or realist perspective, a person negotiating cyberspace and virtual worlds is simply a person sitting at his computer. The information the person posts to an online community board, or uses to form their 3D avatar for Second Life or volunteers during his online travels is simply information that is “out there” in cyberspace connected to the person only insofar as the information is a representation about the person. A virtualist perspective transforms our thinking on these points. It holds that in order to understand privacy in cyberspace, we must first conceive the *virtual person* in cyberspace, and build a framework for privacy protection based on that foundation; this makes sense because personhood has traditionally played a central role in justifying theories, laws and other measures aiming to protect privacy.

I discussed three notions of the person in cyberspace: (1) the virtual person in complete virtual reality environments; (2) the virtual person in 3D virtual worlds; and (3) the virtual person as embodied information. Each of these notions of personhood offered different challenges for a privacy regime, but most importantly, each reconnected the *person* to ideas of informational privacy. From an externalist perspective, the 3D avatar that negotiates virtual worlds is simply a creation of data and information entered by the user external to the virtual world. There is no privacy protection in that information, or for anything the avatar does. Likewise, for the web surfer, information gathered from online e-commerce and other activities is also cut off from the individual and his or her privacy protections. However, a virtualist approach to privacy understands the person *within* cyberspace, such that each of these ideas of virtual persons ought to receive privacy protections, just as our physical persons have traditionally received privacy protections in real space.

Virtualism bridges the divide between privacy and the person in cyberspace. In cyberspace, the virtual person is *constituted* by data and information. If privacy is to be afforded to people from a virtualist perspective, then informational privacy is required by necessity. What would, on the externalist view, be simply a digital record of information collected *about* the person’s avatar or profile in cyberspace, *is* the person in cyberspace on a virtualist approach.

The virtualist approach reconnects informational privacy to personhood, by recognizing that in cyberspace, people take on virtualized form and identity, synthesized and constituted by bits of data and digital information. Similarly, it is much easier to justify privacy protections in our “digital dossier,”²²³ that is, in the information that makes up our online persona, if we understand ourselves as virtual persons in cyberspace constituted by that data and information—if the law defines us as, in Solove’s terms, a “digital person.”

²²³ SOLOVE, *supra* note 50, at 1-2.

I am not a reductionist who believes privacy can be reduced to one simple idea or unified with one definition. But there is a reason why Rubinfeld described personhood as the “reigning explanatory concept” on privacy.²²⁴ Personhood provides a strong conceptual and normative framework for privacy. But informational privacy was set outside that framework, leaving Cohen and others searching for “fundamental values” to justify it. If privacy protects the “integrity” of the person²²⁵ and a virtualist perspective reconnects this idea to privacy in cyberspace, then Cohen’s search, if not over, is at least much more focused and narrowed.

B. VIRTUALIST PRIVACY AND THE CONSTITUTION

1. Against *Whalen v. Roe*: Breathing Life into a Constitutional Right to Cyberspace Privacy

Earlier, I noted that most privacy scholars have little hope for the recognition of a constitutional right most important to privacy in cyberspace, “informational privacy.” Few believe the U.S. Supreme Court will ever expand its passing reference to the idea in *Whalen v. Roe*.²²⁶ Jurisprudence has drawn a “firm line” between “substantive” ideas of privacy relating to issues affecting personhood and informational ones,²²⁷ the former having constitutional protection while the latter not.²²⁸ In fact, I argued that it was this distinction in *Whalen v. Roe*, between informational privacy and the more traditional idea of privacy linked to personhood (i.e. the importance of autonomy and decisionmaking), that has made the recognition of a right to informational privacy unlikely. Much like the predominant conceptual approach to informational privacy, the Court set off privacy in personal information from an entrenched body of constitutional jurisprudence linking privacy to personhood.

After *Whalen v. Roe* two conceptual and jurisprudential lines were formed. On one side were famous privacy cases that tied privacy to personhood like *Griswold v. Connecticut*²²⁹ and *Roe v. Wade*.²³⁰ In both of those cases, privacy was related to ideas about the autonomy, dignity, and decisionmaking of the person, and the need to preserve that space for the person to make fundamental life decisions, particularly about the body (*Roe v. Wade*), without intrusion from government or otherwise. On the other side was the novel idea of privacy in information (enforced by non-disclosure), something the Court had “not previously defined.”²³¹ The Court thus disconnected

²²⁴ Rubinfeld, *supra* note 72, at 739.

²²⁵ Solove, *supra* note 116, at 1116.

²²⁶ See, e.g., Lin, *supra* note 46, at 1089.

²²⁷ Katyal, *supra* note 51, at 239; Katyal, *supra* note 53, at 308.

²²⁸ Katyal, *supra* note 51, at 240-1; Katyal, *supra* note 53, at 308.

²²⁹ 381 U.S. 479 (1965).

²³⁰ 410 U.S. 113 (1973).

²³¹ SOLOVE, *supra* note 50, at 65.

privacy in information *about us* from the central theme of privacy and personhood—privacy in the body and the person. This made it much less likely for a constitutional right to privacy to be later recognized (because it set informational privacy apart from traditional jurisprudence) and also created a conceptual chasm between personhood and informational privacy yet to be bridged.

Not only does the shift to a virtualist perspective bridge the aforementioned normative and conceptual divide, but it also opens the door to the possibility of constitutional recognition. By offering a normative and conceptual means to reconnect privacy in cyberspace (and informational privacy) to personhood, *contra Whalen v. Roe*, we also reconnect informational privacy to more traditional privacy jurisprudence centered on personhood. As noted by Solove, the U.S. Supreme Court has offered a “personhood theory of privacy” in many of its substantive due process decisions centered on privacy.²³² In fact, in 1891 the Court was already linking ideas of privacy to the person, as apparent in *Union Pacific Railway Co. v. Botsford*,²³³ which proclaimed “the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.”²³⁴

Following these ideas of personhood and the “zones” of “personal, marital, familial, and sexual” privacy in *Griswold* and “the right of personal privacy” in *Roe v. Wade*, the Court clearly set out its theory in *Planned Parenthood v. Casey*²³⁵ where, once again, laws controlling abortion were challenged. For the majority, Justice Sandra Day O’Connor wrote:

Our law affords constitutional protection to personal decisions relating to marriage, procreation, contraception, family relationships, child rearing, and education These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment. At the heart of liberty is the right to define one’s own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the attributes of personhood were they formed under compulsion of the State.²³⁶

²³² Solove, *supra* note 116, at 1117 (“The Supreme Court has espoused a personhood theory of privacy in its substantive due process decisions such as *Griswold v. Connecticut*, *Eisenstadt v. Baird*, *Roe v. Wade*, and others.”).

²³³ 141 U.S. 250 (1891).

²³⁴ Solove, *supra* note 116, at 1117 (citing *Botsford*, 141 U.S. at 251).

²³⁵ 505 U.S. 833 (1992).

²³⁶ *Id.* at 851.

This theory of privacy and personhood finds expression in a rich body of constitutional jurisprudence that relates privacy to concerns centered on the person: personal autonomy, intimacy, and decisionmaking, particularly over deeply personal things like our bodies and personal health. Yet none of these ideas have been used by the Court to expand upon the passing reference to informational privacy in *Whalen v. Roe*. The reason, I have argued, is that the court improperly set informational privacy apart from personhood. But a virtualist approach anchors privacy to the *virtual person*, reconnecting concerns of personal autonomy, decisionmaking, and privacy in the context of cyberspace.

In arguing for the recognition of a constitutional right to privacy in information and data tied to individuals in cyberspace, privacy theorists no longer need to rely on unusual ideas of property interests in information, but can, instead, invoke the more common idea of privacy in the person; the only difference is that the persons discussed are *virtual persons*. Privacy follows naturally here—it is tied to our persons, bodies, and identities and, in Justice Sandra Day O'Connor's terms, the decisions we make to define our “concept of existence” in the universe. The only difference here is that the universe is not real space, but cyberspace. The idea that persons in virtual contexts receive privacy protections is not alien to the American constitutional tradition, but an important part of it. As Julie Cohen writes: “A realm of autonomous, unmonitored choice, in turn, promotes a vital diversity of speech and behavior. The recognition that anonymity shelters constitutionally-protected decisions about speech, belief, and political and intellectual association — decisions that otherwise might be chilled by unpopularity or simple difference — is part of our constitutional tradition.”²³⁷ Though some legal commentators will likely remain skeptical about courts finally articulating such a constitutional commitment, the best path to that goal is not in the conceptual divide of *Whalen v. Roe*, but in the normative framework of virtualist privacy. Virtualist privacy illuminates a creative new path toward a broad constitutional right to privacy, which incorporates informational privacy, in cyberspace.

2. Contextualism, not Translation

My argument that privacy theorists should adopt the virtualist perspective in order to justify arguments for the recognition of a constitutional right to informational privacy (necessary for privacy in cyberspace) includes the corollary proposition that theorists should spend less time thinking about the concept of privacy and offering detailed accounts of its constituent parts. Instead, privacy theorists should think more clearly about the subjects of privacy, being people, and how people ought to be understood in the context of cyberspace. These ideas also set out a way of approaching constitutional ideas and concepts in the context of cyberspace. Against Professor Lessig, I

²³⁷ Cohen, *supra* note 76, at 1425.

believe the key to bringing constitutional values to digital contexts is not translation,²³⁸ but what I call “contextualism.”

Virtual and digital technologies are constantly developing and advancing and pose a sustained challenge to legal regimes, particularly constitutions that portend to constrain the conduct of governments and citizens.²³⁹ How can the Constitution preserve liberty and other constitutional values if the context of society and technology changes so rapidly that constitutional constraints are rendered ineffective? Lessig proposes a strategy of what he calls “translation” in order to address this challenge. Translation determines the “original meaning” of a constitutional provision and offers a reading that best preserves that meaning “in the present context,” the context being cyberspace.²⁴⁰ So, with respect to the Fourth Amendment, which originally conceived applied to trespass, Lessig argues that the meaning of the Amendment—to curtail technologies of privacy invasion—means that it should similarly apply to wiretapping and other invasive technologies of today’s world.²⁴¹ This “translates” the constitutional values originally underlying the Fourth Amendment into the context of modern times.²⁴² On one level, my proposals for adopting a virtualist approach to privacy in cyberspace draws on Lessig’s idea of translation. I argue that privacy in cyberspace, which requires informational privacy, can be grounded in traditional constitutional values of privacy based on personhood. I have translated privacy to the context of cyberspace.

But this is not entirely true. Lessig’s metaphor of “translation” does not capture the nature of my approach. I am not arguing that privacy be translated or transformed. The term “translation” implies saying the same thing but in a different language. Instead, I am arguing that privacy not be transformed or translated, just moved and theorized in a different context; there is no translation to a different language, but simply repetition (privacy is good) in a different context (cyberspace). I call this contextualism, rather than translation. The problem with present approaches to privacy in cyberspace is that theorists have failed to take into account the virtualist perspective and how *people* (not necessarily constitutional values) ought to be understood in the context of cyberspace. The central challenge is not to translate constitutional values of privacy, but simply to understand how privacy, traditionally

²³⁸ Lessig, *supra* note 42, at 873 (arguing that translation is “central to cyberspace’s survival as a place where values of individual liberty are sustained”); *see also* LESSIG, *supra* note 7, at 160.

²³⁹ *See* Lessig, *supra* note 42, at 870. Lessig calls this a “codifying” constitutionalism.

²⁴⁰ LESSIG, *supra* note 7, at 160 (noting that translation “aims at finding a current reading of the original Constitution that preserves its original meaning in the present context”).

²⁴¹ LESSIG, *supra* note 7, at 160-61 (discussing Justice Brandeis’ dissenting opinion about the application of the Fourth Amendment to modern technologies).

²⁴² *Id.* at 161.

understood, works in the context of cyberspace. This is a subtle, but important difference.

This might place too much emphasis on Lessig's metaphor of "translation." I agree with Lessig's central point, that constitutional provisions ought to be read *differently* (from, say, their original text) in order to preserve their original purpose of protecting things like liberty or privacy in new contexts. After all, the most likely way a constitutional right to informational privacy will be recognized—even if a court adopts my argument for a virtualist perspective—is through some interpretive strategy like Lessig's theory of translation. There is no provision in the U.S. Constitution providing for informational privacy; rather, the idea must develop out of the "zone of privacy" apparent in the "penumbras" of the Constitution noted in *Griswold v. Connecticut* and *Roe v. Wade*. But *contextual* constitutional interpretation seems more achievable than the more transformative idea of *translating* constitutional values.

C. VIRTUALIST PRIVACY, PUBLIC POLICY, AND CODE

A virtualist approach to privacy in cyberspace offers a new conceptual framework for thinking about legal and technological problems that affect privacy, and also lays the groundwork for greater constitutional recognition for privacy in informational and cyberspace contexts. But there are further benefits relating to public policy, government, and private action on privacy, as well as shaping the future of cyberspace code; these points need elaboration.

1. The State Action Dilemma: Why Constitutional Recognition Still Matters

Critics will point out that a constitutional right to informational privacy, even if recognized by the U.S. Supreme Court, will not solve privacy concerns in cyberspace. Sure, governments, and their great capacity to collect, store, and distribute information about citizens, remain an important, perhaps even central threat to privacy.²⁴³ But in many environments of cyberspace, threats to privacy are posed by private entities, not state actors, to which the Constitution would not apply.²⁴⁴ Of course, a constitutional right will not solve all privacy problems. But that does not mean it would not constitute a key step in the fight for greater privacy protections. I do not intend to rehash all the arguments usually offered as to why a constitutional right to

²⁴³ U.S. federal agencies and departments maintain nearly 2000 databases with records relating to immigration, financial history, welfare, licensing, and many other matters, with records often flowing between the private and public sector. See SOLOVE, *supra* note 50, at 15.

²⁴⁴ Katyal, *supra* note 51, at 381 ("[U]nder the state action doctrine, constitutional guarantees can limit the activities of a private party if the conduct in question is entwined with traditional state functions."); see also Berman, *supra* note 7, at 1266 ("[T]he state action doctrine, in its least nuanced form, rests on the observation that most constitutional commandments proscribe only the conduct of governmental actors.").

informational privacy would be a good thing. This has been done before, in a clear and convincing way.²⁴⁵ Instead, I would like to focus on reasons why a constitutional commitment can have a positive impact on privacy concerns created by non-state action. These reasons have received less attention in scholarship.²⁴⁶ Drawing on what Frederick Schauer calls “First Amendment culture” in the United States,²⁴⁷ a constitutional commitment to privacy, particularly informational privacy in cyberspace, can have a positive impact on privacy concerns beyond its legal enforcement and application to state action.

Each country, writes Schauer, has a “showstopper” for a constitutional or political argument, one that receives more attention, respect and, when deployed, often more success than any other.²⁴⁸ In the United States that argument happens to be free speech via the First Amendment.²⁴⁹ Yet this “free speech” culture cannot be explained by looking to cultural preferences alone, nor, on the other hand, by simply examining the First Amendment and its history of legal and constitutional enforcement. Rather, the value of free speech in America is linked to a deep constitutional *and* cultural commitment; it is a product of a *constitutional culture* of free speech. Hence, Schauer calls it “First Amendment culture.”²⁵⁰ The Founding Generation’s commitment to free speech apparent in the First Amendment, and the provision’s subsequent enforcement in various high profile cases over the years, has helped foster a constitutional culture in broader American society that promotes and preserves free speech and the free movement of ideas.²⁵¹

There is no similar constitutional culture for privacy, let alone data or informational privacy. This has had at least two detrimental effects on privacy protections. First, privacy often conflicts with the

²⁴⁵ See Lin, *supra* note 46, at 1107-18 (discussing the “failure of non-constitutional law” such as tort and statute law in protecting people’s privacy, and arguing that a constitutional right would avoid these problems because it is “permanent” and “inalienable” and would promote privacy protecting measures).

²⁴⁶ *But see generally* Berman, *supra* note 7. Elbert Lin, *supra* note 46, also makes passing reference to the idea. *Id.* at 1122-23.

²⁴⁷ Frederick Schauer, *Principles, Institutions, and the First Amendment*, 112 HARV. L. REV. 84, 111 (1998) [hereinafter Schauer, *Principles*]; see also Frederick Schauer, *First Amendment Opportunism*, in *ETERNALLY VIGILANT: FREE SPEECH IN THE MODERN ERA* 197 (Lee C. Bollinger & Geoffrey Stone eds., 2002) [hereinafter Schauer, *First Amendment Opportunism*].

²⁴⁸ Schauer, *First Amendment Opportunism*, *supra* note 247, at 176.

²⁴⁹ See *id.*

²⁵⁰ Schauer, *Principles*, *supra* note 247 at 111; see also Schauer, *First Amendment Opportunism*, *supra* note 247, at 176.

²⁵¹ Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 U.C.L.A. L. REV. 1149, 1169-70 (2005) (discussing the “importance of the First Amendment to American legal and political culture,” including the “large number” of First Amendment cases decided by the Supreme Court alone over the years, as well as the “voluminous bulk” of First Amendment scholarship).

broad protections and cultural respect accorded to freedom of speech and information. Data and informational privacy regimes or theories that would restrict the flow of data and information often face fierce opposition from speech advocates, usually in the form of the supposed “First Amendment critique.”²⁵² And, in fact, when privacy *has* conflicted with the First Amendment in the past, the latter has invariably won out.²⁵³ Privacy remains at the mercy of First Amendment culture. Second, without a constitutional commitment to informational privacy, there is less general awareness in the broader public about threats to privacy in cyberspace. This means governments, and thus actors in the private sector, have easily ducked their responsibility to ensure privacy is protected in the public interest.

Fortunately, a virtualist approach to privacy opens the door to a constitutional right to informational and data privacy. By reconnecting the ideas of informational privacy to traditional constitutional jurisprudence centered on theories of personhood, the possibility of a broader constitutional commitment to privacy being recognized by the U.S. Supreme Court is that much greater. Such constitutional recognition has benefits beyond the obvious one of limiting government intrusion and overreaching on personal data and information in cyberspace. Paul Schiff Berman argues that constitutional adjudication has important social, political, and cultural benefits outside mere dispute resolution. Adjudication of a constitutional interest in informational and data privacy allows courts to perform an “educative function” by articulating national values and stimulates broader social deliberation of public interest issues like privacy.²⁵⁴ The narratives constructed and promoted by the processes of the law and Constitution contribute and shape social knowledge.²⁵⁵

In advocating a broader constitutional discourse on privacy, Berman’s target is the state-action doctrine. The boundaries set by the doctrine prevent the Constitution from applying to private actors and the threats to privacy they pose on the Internet and in other cyberspaces. But Berman does explain *how* courts might, at the outset, anchor a broader constitutional right to privacy in the Constitution. Courts might agree that constitutional discourse is beneficial, but it needs the tools the get there. The virtualist approach to privacy, if

²⁵² For a discussion and critique of the First Amendment critique see *id.* at 1154-65. See also Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 976-981 (2003).

²⁵³ Richards, *supra* note 251, at 1155 (“[W]hen the First Amendment and privacy have come into conflict in the past . . . the First Amendment has universally triumphed.”).

²⁵⁴ Berman, *supra* note 7, at 1269 (writing that adjudication can allow courts to “perform an educative function by articulating values and constructing narratives” that help construct “national identity” while creating “opportunities for courts to operate as deliberative fora in which difficult political issues are addressed”).

²⁵⁵ *Id.* at 1292 (arguing that the judicial process can also help construct important social narratives by first “enacting a performance in which the society ‘creates, tests, changes, and judges’ the various competing discourses” that make up “social knowledge”).

adopted, offers hope for such constitutional recognition to get where Berman wants to go.

Second, a constitutional commitment to privacy in cyberspace, that is, informational (and data) privacy, imposes greater social and political pressure on governments to take steps—legislative or otherwise—to protect privacy. Paul Schwartz is right to say that privacy “rhetoric” often neglects the positive role the State can and should play in preserving privacy.²⁵⁶ He suggests that governments can advance privacy-enhancing norms, by offering incentives to private and commercial actors for improving privacy protections and promoting a “bandwagon effect.”²⁵⁷ That is, if the State takes a leadership role in protecting the privacy of government data, the general public and non-state actors are likely to follow suit with interest and support.²⁵⁸ Though constitutional recognition is unnecessary for such State initiative, each of these things could help foster a “constitutional culture” of informational privacy, leading to greater cultural awareness and legal significance for privacy claims about cyberspace.

3. Coding the Virtualist Perspective

A constitutional commitment to privacy can also influence those who may be the most important players in the future of cyberspace privacy—not corporations or governments, but the next generation of programmers who will play a central role in shaping and developing the next layers of the “code” of cyberspace in coming years. Lawrence Lessig famously illustrated the importance of computer code to the future of the Internet and cyberspace. Values like liberty and privacy are not intrinsic to cyberspace; rather, they were hard-wired into the architecture of cyberspace at its founding and early development.²⁵⁹ The first generation of programmers was deeply influenced by free speech and the First Amendment culture of the United States. As Lessig observes, TCP/IP protocol essentially codifies the First Amendment into the “architecture of cyberspace.”²⁶⁰ But code is not fixed. The future includes a battle over the types of values to be embedded in the additional layers of code that will govern the direction of cyberspace.

Julie Cohen raises these issues when she discusses “informational privacy by design.”²⁶¹ The architecture of cyberspace is “chosen” and while “privacy considerations” have not been a top

²⁵⁶ Schwartz, *supra* note 56, at 816.

²⁵⁷ *Id.* at 856.

²⁵⁸ *Id.* at 856-57.

²⁵⁹ See Lawrence Lessig, *Code is Law: On Liberty and Cyberspace*, HARV. MAG. (Jan.-Feb. 2000), available at <http://www.harvardmagazine.com/online/0100121.html>.

²⁶⁰ *Id.* at 2.

²⁶¹ Cohen, *supra* note 76, at 1436.

priority so far, this can change.²⁶² Law cannot solve these problems, but it *can* work to “establish a new set of institutional parameters that supply incentives for the design of privacy-enhancing technologies to flourish. Legal protection alone cannot create or guarantee informational privacy. But it is a place to begin.”²⁶³ A constitutional commitment to privacy provides a strong normative foundation to promote privacy-enhancing measures and, in addition, influences the next generation of programmers, the same way the First Amendment influenced the openness of cyberspace code today. The broader advantages and positive implications of a constitutional commitment are felt in those many spaces and forums of living beyond courtrooms and government offices.²⁶⁴

But even if a clear constitutional commitment to informational and cyberspace privacy is never recognized or achieved, virtualist privacy still has positive benefits in this area because it is forward-looking and speaks to people’s experience in virtual environments and cyberspace. Virtual living will become more and more familiar to the next generations of young people, many who will make their way into the field of information technology. The next generation of cyberspace citizens (or netizens) will be raised with greater exposure to technology and cyberspace than any before it and virtualist privacy will speak to their experiences. More than those before, they will understand that for important values like liberty and privacy to find expression in the future structures of cyberspace, software and code must be approached from the virtualist perspective, to take into account the concerns of virtual persons and their interests in liberty and privacy.

VI. MOVING FORWARD: VIRTUALIST PRIVACY IN AMERICA AND ABROAD

The growing body of second generation cyberlaw scholarship, which I have dubbed the New Virtualism, speaks not only to the differential character of cyberspace, but also draws connections between real space and virtual space. This Article is situated within this body of scholarship, offering a new approach to privacy in cyberspace by drawing on the internalist or virtualist perspective.

Some, like Tal Zarsky, doubt the utility of examining privacy rights from a virtualist perspective. He writes that it is “too early” to theorize about independent or distinct privacy rights for virtual persons and identities.²⁶⁵ I disagree. As Zarsky himself notes, there are many

²⁶² *Id.*

²⁶³ *Id.* at 1438.

²⁶⁴ See David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE W. RES. L. REV. 831, 852-53 (1991) (“[T]he purpose of creating a constitutional right to privacy is not to leave data protection solely to the courts, except for the interpretation of the necessary statutes in cases of conflict but to allow individuals to assert privacy claims in various arenas that extend beyond general and specific data protection laws.”).

²⁶⁵ Zarsky, *supra* note 36, at 251 (writing that it is “still too early” to decide whether “virtual personas” should be understood as “extensions” of the self).

people whose online personas are more central to their sense of self than their physical lives in real space. If virtual activities and community are moving in this direction, we ought to be forward-thinking in our approaches to legal and theoretical problems concerning cyberspace, particularly with something as important to the public interest as privacy.

Beyond outlining the origins of the New Virtualism, the primary purpose of this Article has been to shift the predominant focus of most work on privacy in cyberspace away from the concept of privacy itself, to the subjects of privacy, that being persons and how they should be conceived and understood in cyberspace. Privacy theorists need to stop dicing up and over-theorizing privacy and instead think more about the experience of people in cyberspaces, and how privacy ought to work in that context. The virtualist approach to privacy set out here attempts to do this. There may be other approaches that do a better job. My purpose was not to set out an exhaustive account of virtualist privacy, only to offer a beginning framework which, as I have attempted to show, has many benefits. Others might expand on my account, or advance alternatives.

Another future direction for virtualist privacy might include comparative scholarship. Privacy threats in cyberspace are not confined to the United States. Many countries are dealing with domestic concerns about privacy in data and information.²⁶⁶ Since the primary innovation of virtualist privacy is not necessarily the definition of privacy within a unique constitutional or legal culture but understanding how people, the subjects of privacy, are understood in different cyberspace contexts, virtualist privacy could be incorporated into other legal and constitutional regimes. For example, constitutional protections for privacy in Canada under the *Charter of Rights and Freedoms*²⁶⁷ draw on legal norms and concepts apparent in American jurisprudence, like reasonable expectations of privacy.²⁶⁸ In fact, the *Canadian Charter* itself speaks to “security of the person;”²⁶⁹ and this concept has formed the basis of some forms of privacy protections.²⁷⁰ Does section 7 extend to security of *virtual persons*, that is, to provide additional privacy protections for people as they traverse the virtual worlds of cyberspace? The “living tree” approach to constitutional

²⁶⁶ See *id.* at 13 (writing about proposals and solutions to resolve problems of information privacy in other countries).

²⁶⁷ Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982, ch. 11 (U.K.) [hereinafter *Charter*].

²⁶⁸ See Flaherty, *supra* note 264, at 844-47 (noting that in interpreting section of the Charter of Rights, the Supreme Court of Canada adopted the American concept of “reasonable expectation of privacy” set out by the U.S. Supreme Court in *Katz v. United States*, 389 U.S. 347 (1967)).

²⁶⁹ *Charter*, *supra* note 267, § 7 (encoding the right to not be deprived of “life, liberty and security of the person . . . except in accordance with principles of fundamental justice”).

²⁷⁰ Richard B. Bruyer, *Privacy: A Review and Critique of the Literature*, 43 ALTA. L. REV. 553, 579 (2006); see also Flaherty, *supra* note 264, at 844-45.

interpretation in Canada perhaps offers a greater likelihood than the United States for recognition of virtualist privacy and the need for informational privacy in cyberspace.

The externalist/virtualist distinction can be a powerful analytical tool that can and should be used in other contexts. I have used it here to incorporate a “virtualist perspective” on privacy in order to re-frame debates on privacy and perhaps offer a new way forward on these issues. Privacy *is* under threat.²⁷¹ We need to change our thinking sooner rather than later. We must go on.

²⁷¹ Solove, *supra* note 116, at 1089 (“The widespread discontent over conceptualizing privacy persists even though the concern over privacy has escalated into an essential issue for freedom and democracy.”).