THE YALE LAW JOURNAL POCKET PART

JOSHUA FAIRFIELD

# Escape Into the Panopticon: Virtual Worlds and the Surveillance Society

> The Eye: that horrible growing sense of a hostile will that strove with great power to pierce all shadows of cloud, and earth, and flesh, and to see you: to pin you under its deadly gaze, naked, immovable.[1]

## INTRODUCTION

Suppose that you move to a new town. To buy your home, you must allow the developer to install cameras in each room and record all interactions between you and your husband. To use the telephone, you must permit the telephone company to record and retain your conversations. To receive mail, you must allow the mail carrier to copy and index the contents. To access funds, you must permit the bank to record all purchases. Suppose, too, that much of this information can become available to government actors with a simple subpoena rather than the more stringent search warrant.[2] It may sound incredible, but this is the reality for millions of people who live, work, and play in virtual worlds.

The essential irony of virtual worlds is that populations seeking to build new lives away from the public eye are moving into an environment that is subject to constant surveillance. Virtual worlds currently operate like Jeremy Bentham's Panopticon prison.[3] The Panopticon permitted a single guard in the center of the prison to monitor all of the prisoners. The same degree of

1. J.R.R. TOLKIEN, THE LORD OF THE RINGS 616 (Houghton Mifflin 1994) (1954).

2. *See* United States v. Miller, 425 U.S. 435, 444 (1976) (permitting access to bank records with a subpoena and noting the "general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant").

3. JEREMY BENTHAM, THE PANOPTICON WRITINGS (Miran Bozovic ed., 1995).

surveillance exists in virtual worlds. The denizens of virtual worlds are constantly under surveillance by "game gods," the private companies that design, maintain, and administer virtual worlds.[4] The game gods then must comply with government requests for call details, wiretaps, stored chatlogs, and other business records.[5] The result: game gods' cameras are on all the time and the footage reaches law enforcement and the intelligence community.

I argue in this brief essay that as government enters virtual worlds it should respect basic privacy rights. For intelligence and law enforcement purposes, this most importantly includes the question of when government actors can and should access a U.S. person's private communications. Further, I argue that private collection of personal information in virtual worlds is as much of a threat to privacy as government surveillance.

## REASONABLE EXPECTATIONS OF PRIVACY IN VIRTUAL WORLDS

The basic legal regime for privacy prevents the intelligence community and law enforcement from accessing a U.S. person's private communications without a warrant supported by probable cause.[6] The constitutional standard is one of a reasonable expectation of privacy,[7] but courts have had some trouble hammering out what constitutes a reasonable expectation of privacy online.[8] The main point of contention is whether reasonable expectations of privacy are determined by what the government *can* collect or by what it *ought* to collect. The government *can* collect anything. So if the government refuses to respect privacy, then any expectation of privacy is unreasonable.[9] The alternative is for courts to make a normative determination: when citizens reasonably act as

4. One very common example of this monitoring is the retention of chat logs, which the companies routinely record for customer assistance purposes.

5. For wiretaps and access to call details for voice over internet protocol, see Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002(a) (2000). For access to recorded chatlogs via a subpoena, see Stored Communications Act, 18 U.S.C. §§ 2702(b)(2), 2703(b) (2000); and Second Life: Terms of Service, http://secondlife.com/corporate/tos.php at ¶ 6.1 (last visited Nov. 24, 2008).

6. *See* Katz v. United States, 389 U.S. 347, 358-59 (1967).

7. *Id.* at 361 (Harlan, J., concurring) (arguing that an expectation of privacy must be both subjectively held and objectively reasonable).

8. *See, e.g.*, United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002) (denying a motion to suppress evidence based in part on a holding that there is no Fourth Amendment privacy interest in subscriber information). *But see* State v. Reid, 914 A.2d 310 (N.J. Super. Ct. App. Div. 2007) (holding that a person has a reasonable expectation of privacy in ISP account information under the New Jersey state constitution).

9. *See, e.g.*, Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 39 (2004) ("[T]he reasonable expectation of privacy test is circular.").

though their communications are private, courts must select rules that honor those expectations, even if government possesses the technology to access the information.[10] Under this normative approach, the fact that government can wiretap telephones or see through bedroom walls with thermographic cameras does not reduce the expectations of privacy of U.S. persons in bed or on the phone.[11]

In some ways, determining rational expectations of privacy in virtual worlds is easier than determining expectations of privacy over telephone lines, because computer technology allows virtual re-creation of real space. Virtual worlds recreate streets and bedrooms.[12] In the real world, most street-corner conversations are public, and most bedroom conversations are private. Virtual world technology is intentionally designed to make humans act as though the virtual world is, at least in some respects, real. Thus, as a normative matter, when corporations choose to use technology intended to entice humans into acting as though they were safe in their own homes, or privately communicating with friends, the law ought to respect those expectations as it does in real life. I therefore argue that U.S. persons in virtual worlds possess a reasonable expectation of privacy, such that a search of their virtual homes and property should be subject to the warrant requirement of the Fourth Amendment.

## PROTECTING U.S. PERSONS' PERSONAL INFORMATION IN VIRTUAL WORLDS

Government surveillance is only half of the problem. The other half is the untrammeled private collection of data. Companies collect information about consumers to maximize profit or to gain business advantage.[13] Unfortunately, companies often lose control of the enormous amounts of information they

10. *See* Katz v. United States, 389 U.S. at 351-52 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

11. *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001) (holding that the warrantless use of thermal imaging to explore otherwise unobservable details of a private home is a violation of the Fourth Amendment); Katz v. United States, 389 U.S. at 359 (finding a reasonable expectation of privacy in conversations over telephone lines).

12. *See generally* EDWARD CASTRONOVA, SYNTHETIC WORLDS: THE BUSINESS AND CULTURE OF ONLINE GAMES 6-9 (2005) (describing the nature of worlds created through video game technology).

13. DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 623 (2d ed. 2006) ("An entire industry has arisen devoted to the creation of gigantic databases of personal information . . . .").

have gathered, which threatens U.S. persons' privacy.[14] Congress has already begun to act in response to the threat of massive collection of U.S. persons' data by companies that do not carefully protect that data.[15]

But the more people live out their lives in virtual worlds, the more information can be data mined. Not only economic information like credit card numbers can be recorded in virtual worlds. The false anonymity of novel online environments has caused people to move their intimate lives online, where every act can be monitored.[16] Eventually, every movement, every gesture in virtual worlds will be tracked and processed by private companies. The government should take the lead in protecting consumer privacy from private invasion by extending enforcement of law on data leaks[17] to virtual worlds, by enforcing existing law requiring informed consent prior to the collection of personal information,[18] and by enacting new law creating property rights in personal information so that consumers will have adequate control if they decide to sell their information.

## CONCLUSION

As people move their lives online, courts should recognize that rights move with them by articulating a reasonable expectation of online privacy. Rights to privacy do not stop at the gateway to virtual worlds. And the fact that surveillance in virtual worlds can be ubiquitous does not indicate that it should be. There is a serious danger that courts will determine that every aspect of a person's virtual life can be collected by private companies and passed along to government actors subject to less stringent requirements than probable cause. This would be an unfortunate result: either a vibrant and important

14. Over 236 million records have been compromised in the United States since 2005. *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Nov. 25, 2008).

15. *See, e.g.*, Aaron Ricadela, *Congress Takes Aim at Spyware*, BusinessWeek.com, June 18, 2007, http://www.businessweek.com/technology/content/jun2007/tc20070618_693312.htm.

16. *See* PETER LUDLOW & MARK WALLACE, THE SECOND LIFE HERALD: THE VIRTUAL TABLOID THAT WITNESSED THE DAWN OF THE METAVERSE 127-134 (2007) (detailing sexual practices in virtual worlds). These sexual practices can be monitored and disclosed just as any other activity in a virtual world may be.

17. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915 (2007) ("The latest example of regulation through disclosure is a requirement that companies notify individuals of data security incidents involving their personal information.").

18. *See, e.g.*, CAL. FIN. CODE § 4052.5 (West 1998 & Supp. 2008) (requiring "explicit prior consent" before financial institutions may share customer information).

technology would fail, or people would give up all privacy just to use the technology.

Even if government actors take privacy in virtual worlds seriously, however, there remains the problem of private data collection. Virtual worlds are enormous cameras. As people live more of their lives online, they will provide more data that will then be collected and processed. Further, the rules that courts and legislators craft for virtual worlds will soon be applied to the real world because the two will begin to overlap. The next generation of computers will be small enough to wear, and powerful enough to record and parse everything around them. We will all record each other's every action. The Panopticon is a virtual world problem, but it will not remain so for very long.

*Joshua Fairfield is an Associate Professor of Law at Washington & Lee University School of Law. He writes and speaks on the governance and economics of virtual worlds.*

Preferred Citation: Joshua Fairfield, *Escape into the Panopticon: Virtual Worlds and the Surveillance Society*, 118 YALE L.J. POCKET PART 131 (2009), http://thepocketpart.org/2009/01/19/fairfield.html.