
Video Games “See” into Players’ Living Rooms

Video game manufacturers are racing to provide ever more realistic gaming experiences that allow players to perform natural physical movements—for example, dancing or jumping to control a character in a game rather than pressing a series of buttons on a video game controller. The trade-off is that while such games are more immersive because they make natural movements part of play, they are also more invasive since these seeing devices are analyzing gamers’ bodies, behaviours, and environments and thus capitalizing on a rich source of personal information.

One video game system that has used this novel technology is Microsoft’s Xbox 360. Microsoft’s Internet-connected video game system, released in 2005, uses a service known as Xbox LIVE to let users play games with others online, purchase games from a digital marketplace, and keep track of their gaming statistics using digital trophies known as “achievements.”

Although the Xbox 360 has a variety of accessories, including a microphone for voice chat and a webcam for video streaming, its most interesting attachment is the Kinect, a sensor released in 2010 that can “see” a player’s body and distinguish it from furniture and even other people. The Kinect projects infrared light onto the space in front of the device. That light is reflected back by human bodies to an infrared sensitive camera on the Kinect, which tracks movement

to a form of target marketing that is becoming more focused because of the greater ability to connect this information with personal data culled from other aspects of customers’ lives.

After brushing her teeth, Farah checks her Facebook account. She is officially too young to have such an account, but she and most of her friends lied about their age when registering and are now regular users. Every bit of information that Farah reveals about herself on Facebook—every event, song, or show that she “likes,” every status update and every picture—becomes part of the enormous data warehouse that the company sells to third parties. In the event of an emergency, police and security officials would also have access to the information on her page. Today, however, not much is happening, except that her friend Josh is bragging about his new toy car. Because he identifies the toy manufacturer by name, his comments will be automatically culled by firms that conduct online “data scrapes,” invisibly amassing and combining the comments of thousands of users about particular topics, products, or services. These firms then sell these data to companies

and translates players' bodily movements into the game world. The Kinect has proven so vital to Microsoft's business strategy in video game systems that the device will be included in successor versions of the Xbox.

This seeing capacity of the Kinect is also used to monitor emotional responses to marketing. Should Farah or her brother, or any real-world child, decide to watch a video or television program through the Xbox 360, the Kinect plays an advertisement called a "NUad" prior to the video. During this commercial, the system monitors users' reactions to see if they are paying attention to the advertisement. Microsoft then sells this data and those from millions of other users—including players' age, race, and gender gathered by the Kinect and Xbox LIVE, along with information about player behaviour during the commercial—to advertisers for market research. Microsoft has also patented the ability to use the Kinect to prevent people from breaking "terms of use" rules that govern how many people might watch a video or play a video game. For example, if the Kinect senses more people watching a video than are allowed under such rules, it will turn the video off. Does Microsoft have every right to enforce these rules, or is the increasing potential for sensing technologies to enforce digital rights management in physical space blurring the boundaries between Microsoft's corporate and marketing policies, on the one hand, and the living rooms of its customers, on the other?

eager to read citizens' candid comments about products or policies. These same firms also collect online comments about people's views on policies and social issues, which they sell to political strategists.

As her best friend, Ariel, is not yet allowed on Facebook, Farah uses Gmail to send Ariel a funny picture of the family's dog. Again, although the rules for Gmail say that they are too young to have an account, Farah and all of her friends just lied about their age when registering. What she does not know is that when she communicates by email, her correspondence is subjected to different levels of automated scrutiny by global security agencies that monitor the flow of email. Should she contact suspicious people or use specific words or word combinations, her correspondence could be flagged for still greater scrutiny and follow-up by security officials. Her father often observes that, as a nuclear physicist educated in Iran, it is likely that his and all other family members' messages are routinely read.

Stepping out the door, Farah contemplates how different things look on this warm spring day compared to the image of their street on Google Street