JOURNAL OF COMMUNICATION

Journal of Communication ISSN 0021-9916

ORIGINAL ARTICLE

Who's Watching Whom? A Study of Interactive Technology and Surveillance

Lee Humphreys

Department of Communication, Cornell University, Ithaca, NY 14853, USA

Information technology and new media allow for collecting and sharing personal information at unprecedented levels. This study explores issues of privacy and surveillance with new interactive technologies. Based on a year-long field study, this project examines how people think about privacy and surveillance when using mobile social networks. Using the case of Dodgeball, the study found that most informants were not concerned about privacy when using the mobile social network because they felt they were in control of their personal information. There was, however, evidence of 3 kinds of surveillance present in everyday usage of Dodgeball: voluntary panopticon, lateral surveillance, and self-surveillance. This study sheds light on the everyday conceptions, meanings, and activities associated with surveillance, privacy, and interactive technologies.

doi:10.1111/j.1460-2466.2011.01570.x

Mobile phones are an increasingly important tool for communication. In the United States, over 302 million people are mobile phone subscribers (CTIA, 2011). Mobile phones are beginning to resemble computers more than they resemble landline telephones. With the advent of the iPhone and other "smart phones," mobile phones are becoming tools used to access information and services previously accessed exclusively through desktop and laptop computers. A study by the Pew Internet and American Life Project (Anderson & Rainie, 2008) predicted that by 2020, most people in the world will access the Internet through mobile devices.

New social networking services for mobile phones have been developed which purport to allow people to create, develop, and strengthen social ties. Much like social network sites on the Internet (boyd, 2004; boyd & Ellison, 2007; Ellison, Steinfield, & Lampe, 2007), these mobile services provide users with another platform to connect with old friends and meet new friends. Social networking services for mobile devices often rely on users sharing their location as well as other personal information with friends and other users of these services. Thus questions arise about how these

Corresponding author: Lee Humphreys; e-mail: lmh13@cornell.edu

mobile users manage expectations, norms, and understandings about privacy and surveillance when broadcasting personal and locational information.

This study explores how people think about privacy issues and personal information when using new interactive technologies. On the basis of a year-long qualitative field study, this article examines how issues of privacy and surveillance are experienced when using digital interactive services, such as mobile social networks. This article begins by defining surveillance and privacy and exploring these concepts with regard to information technology. Then the case study and methodology are explained. Next, the results describe how people articulated privacy concerns about using a mobile social network and explore the evidence for three kinds of surveillance that manifest in mobile social network use.

Privacy and surveillance

The rise of information technology brings about many issues with regard to privacy and surveillance. Privacy and surveillance are often presented as counterpoints when discussing issues of personal information and new technology. Privacy has been defined as the ability to control what information about oneself is available to others (Westin, 2003). When one cannot control what information about oneself others know, one may be open to surveillance by others. Lyon defines surveillance as "any collecting or processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been gathered" (2001, p. 2). Inherent to the definition of surveillance is the power or influence over others. Asymmetry is an important differentiating factor between monitoring or watching and surveillance (Andrejevic, 2006). Part of the power of surveillance is that people whose personal data are collected or observed may not know when or if they are being watched.

Twenty years ago, Oscar Gandy (1989) argued that the use of new information technologies by corporate and state bureaucracies leads to increased surveillance in society. Like Poster (1990), Gandy suggests that information technology and the growth of databases create an asymmetrical monitoring of behavior. Drawing on Bentham's concept of the panopticon (Foucault, 1977), Gandy (1993) demonstrates how information technology facilitates the surveillance by an unseen corporate and bureaucratic observer who can not only commodify the personal information of those observed, but also use such information to inform practices of social control and discrimination. Such information technology "involves the collection, processing, and sharing of information about individuals and groups that is generated through their daily lives as citizens, employees, and consumers and is used to coordinate and control their access to the goods and services that define life in the modern capitalist economy" (Gandy, 1993, p. 3). Thus the monitoring of individuals through information technology allows for people and groups to be sorted into categories based on their presumed economic or political value and those deemed more and less valuable may be given differing economic and political opportunities.

As Lyon (2001) argues, the information society is a surveillance society. Information and computing technologies both facilitate but also necessitate the collection

of personal information. Information technology databases allow for the integration and layering of different kinds of information from different sources. The most important aspect of this point is that it allows those who control the databases (often corporate or government entities) to know more about individuals than they may know about themselves. This coupling of information highlights behavioral and cognitive tendencies which people may not be aware of. This information can also be commoditized and potentially used for discriminatory activities (Gandy, 1993).

Privacy and surveillance have long been concerns of scholars of interactive media. Previous studies have explored privacy concerns when using particular interactive technologies such as cable television (Kay, 1978; Vidmar & Flaherty, 1985), electronic banking (McLuhan & Powers, 1980; Poster, 1990), TiVo (Elmer, 2003; Andrejevic, 2007), and the Internet (e.g., Elmer, 1997; Fox et al., 2000). These studies suggest that the use of interactive digital technologies leads to a decrease in personal privacy because people do not have control over their personal information. Interactive technologies rely on people disclosing personal information in order to provide them with services. People willingly share their personal information because they derive some sort of benefit from these interactive, information-based services. Thus reinforcing the notion that the information society is a surveillance society (Lyon, 2001).

Three kinds of surveillance

In addition to the traditional notion of surveillance that is characterized by its nontransparency by an authority such as the government, three other kinds of surveillance have been identified in the literature: voluntary panopticon, lateral surveillance, and self-surveillance. Voluntary panopticon refers to the voluntary submission to corporate surveillance or what Whitaker (1999) calls the "participatory panopticon." A voluntary or "participatory" panopticon differs from older systems of surveillance in that it is consensual (Whitaker, 1999). People willingly participate in the monitoring of their own behavior. The voluntary panopticon is based on a consumer society where information technology allows for the decentered surveillance of consumptive behavior. People willingly participate in such monitoring because they believe it is of benefit to them.

Lateral surveillance is the asymmetrical, nontransparent monitoring of citizens by one another (Andrejevic, 2006). With the advent of the Internet and interactive media, people have similar technological capabilities previously held exclusively by corporate and state entities. As such, citizens can monitor other citizens' behavior through nonreciprocal forms of watching. Everyday people can search for information about other citizens without their knowledge or permission.

The last kind of surveillance is self-surveillance. Meyrowitz (2007) defines self-surveillance as "the ways in which people record themselves (or invite others to do so) for potential replaying in other times and places" (p. 1). Technologies such as video cameras and cameraphones allow people to capture aspects of their lives to replay later. The ability to record oneself can lead to the scrutiny of mundane behavior, which can fundamentally change one's understanding of that behavior or event. The recorded

behavior has power over the lived experience because exposure to the recorded behavior can replace or alter one's understanding of the event based on one's lived experience of it. Therefore power implicitly functions within Meyrowitz's concept of self-surveillance insomuch as new interactive technologies, such as mobile social networks, allow users to "see" things about their behaviors they previously could not perceive and changes their understanding of their own tendencies and behavior.[1]

Case study

This article is based on a case study of Dodgeball. Dodgeball was a mobile service owned by Google that distributed location-based information of users so that people could meet up at venues within cities. Similar to a social network site, Dodgeball allowed users to set up publicly articulated social networks of friends so that they could broadcast their location to these individuals' mobile devices. For example, when users got to a bar or cafe, they could "check in" by sending a text message to Dodgeball such as "@ Irish Pub." Dodgeball then broadcasted their location via text message to people in their Dodgeball network. The system also allowed members to send "shouts" or general text messages broadcasted among Dodgeball friends, such as "Roof party tonight my place 9 pm 'til whenever." Shouts could be used like a check-in to facilitate meeting up at places not in Dodgeball's venue database or for whatever other reason users might want to broadcast messages to their Dodgeball network of friends (such as jokes, celebrity sightings, etc.).

Founded in 2000, Dodgeball was one of the first commercial mobile social networks and was available in 22 cities in the United States. It was free to use; however, users were charged by their mobile carriers for each text message they sent and received through Dodgeball (unless they had signed up for an unlimited text messaging plan). Dodgeball did not use GPS (Global Positioning System) but required users to actively text message their location to Dodgeball.

Dodgeball was officially shut down in January 2009, but Google launched Google Latitude which allows users to "see where your friends are right now" on a Google Map (http://www.google.com/latitude/intro.html, consulted March 27, 2009). The Dodgeball founder also went on to start foursquare, another location-sharing mobile social network, in 2007. Like Dodgeball, Google Latitude and foursquare offer users the ability to share their locations with friends via their mobile phones or their computers. Google Latitude and foursquare are more technologically advanced than was Dodgeball. As a mobile service, Dodgeball relied on text messaging to send location information to and from users. Google Latitude and foursquare use mobile smart phone technology so that users can see a map of their friends' locations via their phone rather than receiving text messages with their friends' locations. The location-sharing function of Dodgeball, Google Latitude and foursquare is fundamental to each service and very similar.

Methodology

On the basis of a year-long study (2005–2006) using participant observation, user observations, and in-depth interviews, this article explores Dodgeball use and how it relates to privacy and surveillance. Twenty-one in-depth interviews were conducted with Dodgeball users from seven cities throughout the United States.[2] Because the Dodgeball system did not allow users to easily send messages to people who are not "Dodgeball friends," I initiated contact with Dodgeball's founder, Dennis Crowley, to ask if he would help recruit informants. Crowley sent recruitment e-mails to top users in several cities. In addition, I used snowball sampling based upon those interviews. In total, I interviewed 13 users through an introduction from Crowley and 8 users with a snowball sample from the original 13. While I was originally interested in the issue of privacy on Dodgeball when collecting data, the various conceptions of surveillance did not emerge as a salient topic until after the data collection had been completed. Therefore I was not able to probe the topic directly with most of the study participants. In addition, I analyzed messages sent among a group of Dodgeball users sent during a week-long period in October 2006 in order to explore trends in timing, language, and proximity. I also interviewed Crowley to understand the background and context of Dodgeball as a mobile social network service.

The demographics of my Dodgeball informants varied by several characteristics. I interviewed 9 women and 12 men, ranging in age from 23 to 30. Geographically, they lived in Chicago ($n = 1$), Los Angeles ($n = 2$), Minneapolis ($n = 4$), New York City ($n = 9$), Philadelphia ($n = 3$), San Francisco ($n = 1$), and Seattle ($n = 1$). I conducted fieldwork in Philadelphia, New York City, and Minneapolis and therefore was able to interview more users in these cities. Other interviews were conducted over the phone. My informants' Dodgeball networks ranged in size from 1 friend to 149 friends. The mean number of Dodgeball friends for my sample was 40.38 ($SD = 37.41$) and the median was 24 friends.

Most of my interviewees (18 of the 21) considered themselves as highly active Dodgeball users. Five of the 13 informants recruited through Crowley had been top users with the most check-ins in their respective cities within a particular month. This sample is not a representative sample of Dodgeball users, but a sample of mostly enthusiastic early adopters. Nevertheless, studying the activities of this group of users is an important first step in exploring the ways in which people embed social meaning in mobile social network use.

Throughout this project, I used a naturalistic and interpretive approach in order to understand the perspectives of the Dodgeball participants (Lofland, Snow, Anderson, & Lofland, 2004). Using the constant comparative method (Glaser & Strauss, 1967), I analyzed interview data and fieldnotes to identify recurrent themes. QSR's N6 software was used to categorize and compare findings across informants. Throughout the course of the year, I did have multiple points of communication, interaction, and observation of users. The communication exchanges I had with informants about the mobile social network were both direct and indirect. I was

able to directly gather data about Dodgeball through observing user behavior (e.g., what people put in their public profiles or where I observed them using the service). In addition, some of the informants ($n = 7$) added me as a friend on Dodgeball, so I was able to observe their Dodgeball behavior through their Dodgeball text messages. Most of the data about usage, however, was collected indirectly through people's formal self-reports during interviews. While I have little reason to believe that informants lied to me about their usage or motivations, I cannot necessarily verify their responses. It is possible that informants may have said things about how they use these systems so as to try to impress me. This performance, however, is just as important to me because it conveys expectations, attitudes, and beliefs about how mobile social networks are supposed to work. In addition to formal self-report about usage, I gathered data about mobile social networks from interacting with informants more informally. The conversations and exchanges that occurred before and after the formal interview also provided further information about the culture of Dodgeball. I was able to member check many of my findings both with the founder of Dodgeball as well as five of the informants as a means validating my research. While my observations and interviews may be influenced by my presence, by immersing myself as a member and a researcher, I was able to gather data both formally and informally, directly and indirectly. Altogether these combined methods have helped to provide a richer, fuller picture of how mobile social networks work in grounded practice.

Results

Privacy

I asked informants if they had any thoughts or concerns about privacy when using Dodgeball. Based on their responses, all the Dodgeball informants I interviewed implicitly defined privacy as privacy from other users or people and not privacy from corporate or bureaucratic entities. Informants were also generally not concerned about privacy for one of two reasons: (a) because they felt they had control over their information and to whom it was sent and (b) because they were experienced and savvy Internet users.

Some Dodgeball informants suggested that they actively controlled their privacy because they controlled when, where, and to whom this information is sent.

> One of the things I love about Dodgeball is that it's elective. A lot of people say things like, when they're not really thinking about it, they say things like, "Well, geez, people just know where you are. Isn't that kind of creepy? Can't people stalk you?" And it's like, no. You've chosen who you want to communicate this to and you've chosen when you want to communicate it. So it's entirely in your power. (Nick, New York City)

Because Dodgeball users had the power to choose when to communicate and to whom, informants such as Nick were not concerned about privacy. Similarly, Leonard felt that he is a savvy Internet user who has control over the sections of his life for which he used Dodgeball.

> I feel like I'm a pretty intelligent user of online tools. Like, you hear about all these kids that go on, younger kids, that put on a whole lot of information and they're used to this idea that you fully dump your personality, irony and awe online. And I mean, I've been through that and I've come out the other end wiser. I use Dodgeball for a certain section of my life that has to do with my casual social life. There's nothing interesting that anyone could mine from my check-ins map. Like I said, my real friends are the one on my friends list. Because I don't just serial add, to use the MySpace term, because I'm not a serial adder on Dodgeball, everyone that I would see as a friend-of-friend has been screened by a real friend. So I'm not super concerned because of my usage patterns and my friends, because I'm kind of discretionary with my network. (Leonard, Los Angeles)

Informants like Leonard felt they were in control of their information on Dodgeball and were thus not concerned about privacy issues when using the system. The Dodgeball Web site explicitly suggested that one way users could control their privacy was by carefully selecting the composition of their Dodgeball network of friends. A line from the Dodgeball privacy statement indicated this: "You can control how certain information is displayed by selectively choosing your friends" (Dodgeball, 2005). Users like Leonard heeded Dodgeball's advice about maintaining privacy through careful friending.

Other informants such as Deirdre were not concerned about privacy on Dodgeball because they believe they are good judges of character after having been online for many years.

> Interviewer: One of the things we didn't really talk about yet is this issue of privacy. Have you ever been concerned about it in terms of Dodgeball?
>
> Deirdre (Minneapolis): No. I've been online for close to 10 years and I've met hundreds of people whom I originally met online. And I've encountered some really weird people. But so far I've never had a situation turn out dangerous for me or scary. In general I tend to take everything with a grain of salt in terms of online predators and stuff. I'm a pretty good judge of character. I'm a pretty good judge of character online. And also I'm just loud and don't care what anyone thinks of me so. I'm pretty much, "Ah, whatever." I'm not afraid to leave if the situation gets scary. The situation's never gotten scary though. No, I have no fear about it.

Deirdre was not concerned about privacy on Dodgeball because she believes she has learned how to be savvy online. Privacy on Dodgeball, for Deirdre, was implicitly defined as privacy from dangerous or scary users. Because of her experience interacting with others online, she was not concerned about scary situations that might have arisen through her Dodgeball use.

There was one informant who suggested that Dodgeball could raise privacy concerns for some people. Kirk explained that Dodgeball may not be for everyone.

> I think you have to have a weird sense of privacy, where you're not paranoid about people following you around or stalking you. Because if you think the idea of people knowing where you are is scary, then I think you're not the kind of person who's gonna be into [Dodgeball]. And it's strange that there are quite a few people like that. Even people who don't have cellphones. Like a lot of people don't have cellphones for that same reason. They don't want to be contacted wherever I am. And so Dodgeball is one step beyond that. Not only can I be contacted, but they will know where you are. And the real time aspect of that, I dunno, can be a little scary at first, until you realize that it's all just for fun and everyone's friends. (Kirk, Seattle)

Kirk acknowledged that the amount and kind of information collected and disseminated through Dodgeball could be scary, but because such information was only going to "friends" and it was not worrisome. However, such information could be shared with strangers. Because Dodgeball cataloged all check-in messages, it offered Rich Site Summary (RSS) feeds of members' check-ins so that members could share their check-in information on their blogs or elsewhere. While most Dodgeball users did not use the RSS feeds, Kirk did use this on his personal Web site and reflected on how sharing this information may change norms of privacy.

> [Dodgeball has] an RSS feed for all your check-ins. So, I'm sort of opposite from the kind of person who's hyper concerned about privacy. I like to publish as much as possible and see what evolves out of that. So every check-in that I have ends up on my website. So anyone, even if they're not my friends, can know where I am. And it's been interesting. I just want to see what happens with this publicity. Cuz (sic) I think a lot of publicity and privacy concerns have been created because that's the way it's always been. Just because no one ever has been able to tell strangers where people are, [it doesn't] make it a private matter. I don't care. Every time you go out, you're in a public place. There's no secret about where you are to the people who are in the bar with you of course. Complete strangers will know where you are of course because they're there with you. That's the same way it is with the website. Complete strangers will know where you are because they're in your RSS feed or something. I'm really curious to see where that sort of information goes. (Kirk, Seattle)

Kirk's RSS feed of his Dodgeball locations was a social experiment to see what happens when he broadcasted information about himself as often as possible. When I interviewed him, he had received no feedback from anyone besides Dodgeball friends about his Dodgeball use. His experiment of publicizing his location had not reached beyond his immediate social circle.

For my Dodgeball informants, the overwhelming sentiment regarding privacy was twofold. First, privacy was implicitly defined as privacy from other users. Second, privacy was not typically a concern because users felt they had control over their information. Nevertheless, while Dodgeball users controlled which Dodgeball

members had access to their social–locational information, they did not have control over their personal information by corporate entities.

Voluntary panopticon

As much as Dodgeball members were telling their friends where they were, they were also telling Google where they were. Every time a Dodgeball member sent a check-in message or a shout message, they sent it to Google. Such behavior illustrates a voluntary submission to corporate surveillance or what Whitaker (1999) calls the "participatory panopticon."

Like other participatory panopticons, the benefits of using Dodgeball were tangible. For the Dodgeball members I interviewed, it facilitated sociality. Informants indicated that Dodgeball made it easier to coordinate meeting up. Communication on the system also reinforced social bonds (Humphreys, 2007). Additionally, some members felt Dodgeball was a cheaper, more efficient way to communicate with groups of friends than to contact each friend individually. The benefits of using Dodgeball were apparent and immediate to these active members.

Some Dodgeball informants suggested that one of the reasons why they liked Dodgeball over other services was because it was an opt-in system. Users had to actively submit their social–locational information to Dodgeball rather than being tracked by GPS.

> I like having my privacy when I want it. I'm very big about not being tracked or logged and you know recorded without me knowing it's happening. And so with Dodgeball it's cool. As opposed to something that automatically puts you on a map and logs you in. It's great for me to be able to say, I want people to know that I'm here. But if I'm somewhere else and I for some reason don't want people to know, I just don't check in. Nobody needs to know that I'm sitting at work on a Tuesday afternoon. Things like that. I like that you have to take an action for it to get logged as opposed to it being all automatic. (Dean, Chicago)

For Dean, who is a computer programer, the fact that Dodgeball did not automate its service afforded him a sense of privacy, which he liked. He liked feeling as if he had control over his information; he liked volunteering his personal information when he found it beneficial to do so. Despite this *sense* of privacy, however, by participating in an interactive system where one's behaviors and interactions are mediated through a central server that can then be linked to other databases, Dean's participation on Dodgeball feeds into what Andrejevic (2007) has termed the "digital enclosure," "an interactive realm wherein every action and transaction generates information about itself" (p. 2). The promise of interactivity leads to the participation by everyday people in a system where the traditional work of marketers is replaced through the data mining of transaction-generated information. Within this digital enclosure, Andrejevic (2007) argues that participation in interactive media is an "invitation to participate in one's own manipulation by providing increasingly detailed information

about personal preferences, activities and background to those who would use the knowledge to manage consumption" (p. 242). By volunteering up his personal information so as to coordinate meeting up with friends, Dean submitted personal and locational information to Google. Dodgeball users like Dean were doing the work of an interactive surveillance society.

While some Dodgeball informants enjoyed the autonomy of having to proactively contribute to the system, other Dodgeball informants would rather give up this autonomy of interactive participation. These Dodgeball informants suggested that they would rather submit to automated tracking of their movements so that they do not have to bother to check in.

> Ideally you want some sort of asset, you know when you go out at night, which would just automatically check in from every bar that you crawl to. In a pure, localized software, wireless environment, you could do things like that. Dodgeball is not automatic. It requires a lot of effort on someone's part. (Irwin, Los Angeles)

Irwin felt that Dodgeball was a lot of work and would rather have that work be automated through a GPS-like system. Taylor felt similar to Irwin. "It's kind of a pain to be constantly checking in everywhere. So they could integrate some sort of GPS homing device. And so you don't have to go through that process of manually typing in all those names" (Taylor, New York City). Both Irwin and Taylor thought that automating the Dodgeball check-in process would make it easier for users. This is part of the reason why a voluntary panopticon is so powerful. People willingly submit to surveillance for the sake of convenience.

It is important to note that the Dodgeball members I interviewed did not express any concerns about surveillance when using a mobile social network. Nor did they bring up issues of surveillance at all. No one mentioned state or corporate surveillance during any of the interviews. As Whitaker (1999) points out, this is not terribly surprising because such concerns are generally intangible. This kind of surveillance, however, could potentially lead to discrimination and social control as has been demonstrated with other examples of interactive technology (Andrejevic, 2007; Gandy, 1993). Nevertheless, it is unclear how exactly Google used the information collected through Dodgeball.

A potentially relevant factor that may help to interpret this finding is the degree to which Dodgeball was actually integrated into Google. When Google first acquired Dodgeball, there was plenty of speculation that Google would integrate Dodgeball into their other services, and thus its many forms of targeted advertising (e.g., Shirky, 2005); however, there was little actual evidence of this. Besides the replacement of the Dodgeball log-in with a Google log-in and the replacement of the Dodgeball privacy statement with Google's official privacy statement, there was little evidence of any strategic integration of Dodgeball with the rest of Google products

and services. For example, Dodgeball was not cross-promoted on any of Google-owned webpages, nor was it featured on the primary product webpage of Google. Additionally, the founders of Dodgeball eventually quit Google two years after their acquisition because they felt that Google bought them and then did nothing with them (Crowley, 2007). This, coupled with the disintegration of Dodgeball in January 2009, leads me to believe that Google did not strategically integrate Dodgeball or the consumer information collected through Dodgeball into their other services. That said, Dodgeball was technologically integrated via the log in and legally integrated into Google through its privacy statement. Therefore while it is unclear the degree to which Google strategically used Dodgeball data, according to their privacy statement Google and all Google's partners had access to all Dodgeball user social–locational information. In addition, Google's (2009) mobile privacy statement indicates that location information of Google Latitude users is collected, stored, and merged with other Google Account information. "If you use Google Latitude on a mobile device, in addition to other information, we collect battery life information and tie it to your Google Account" (Google, 2009). According to this mobile privacy policy, such customer information is used to "process and personalize" users' requests. This suggests that your search results may be influenced by where your location is tracked.

Lateral surveillance

Dodgeball also facilitated a kind of lateral surveillance where network members monitored the communication and behavior of other network members (i.e., their friends). As a communicative system, Dodgeball relied on mutual monitoring—friends telling each other where they are through Dodgeball so that they can meet up. However, not all members of the network used the system in the same way. Sometimes there was asymmetrical use of Dodgeball where one member checked in on Dodgeball and another member would not. This asymmetry is the difference between surveillance and monitoring (Andrejevic, 2006). Elicia in New York suggested that there were people in her network who generally do not check in on Dodgeball, but still receive the messages. "There's also a group of people who are more like the eavesdroppers who never send out ever, but they always want to know where people are . . . . They still find it interesting to observe, but they don't want to participate" (Elicia, New York City).

When people observe each other's mediated behaviors in an asymmetrical manner, such as Elicia describes, Dodgeball could become a tool, not for social interaction and coordination, but for lateral surveillance. "Interpersonal interaction always contains an element of mutual monitoring, but the deployment of interactive networked communication technology allows individuals to avail themselves of the forms of asymmetrical, nontransparent information gathering modeled by commercial and state surveillance practices" (Andrejevic, 2006, p. 398).

Continued lateral surveillance on a mobile social network like Dodgeball may ultimately weaken the network. If there are too many people "eavesdropping," then there may be little value for other people to use it and the network can break down. Taylor from New York City reflects on this point:

> There are a few people [in my Dodgeball network] that don't even use the service really but they're a part of my network and they just sort of sit back and get texts from me all the time. And so they know where I'm at, but they don't really contribute which is kinda weird. Because they don't actively contribute. Because they're more browsing, seeing where people are at rather than posting their own whereabouts. But there are definitely quite a few people like that, that just sort of sit back and take things in . . . . But that's how the network breaks down, when people don't contribute. (Taylor, New York City)

If people did not actively contribute to their Dodgeball networks, the value of it for those who did contribute decreases. This may ultimately hurt the growth and sustainability of the mobile network. For example, two members I interviewed in Philadelphia were in each other's Dodgeball network. They had each checked in a couple of times, but no one ever was able to meet up. Eventually they stopped using the network altogether because they were never able to leverage its benefits.

In addition to just eavesdropping, lateral surveillance could potentially also lead to stalking. In the last 15 years, cyberstalking has become a societal concern (McFarlane & Bocij, 2003). Overall, however, the Dodgeball informants I interviewed were not concerned about stalking on the network.

> I just figure there are some people who are just more into checking in all the time and some people are lazier. So if you have someone who's lazy and never checks in, are they surveying me? Not really, I'm willingly checking in. There's no surveillance aspect to it at all because it requires that a user input a check in. There is no kind of surveillance. I never feel like it's a stalking or whatever. You know, and in my circle, it's at least 50% female. Although you know that's probably not reflective of Dodgeball in general because I'm sure girls are afraid of the stalking aspect. You know, when you sign up for Dodgeball they explain all the ground rules. They do go way out of their way to try to calm people's concerns. They go, ''Look, we've prevented all these ways so that no one can really stalk you.'' And you know that's good enough for me. But then again I've never really been stalked so I can't say it's high on my priority of what I'm afraid of. I'd probably be more complimented. ''Oh you're stalking me? That's so cute!'' (Irwin, Los Angeles)

Irwin was not concerned about stalking on Dodgeball because he knew to whom the information was sent and believed that the reason why people on his network did not contribute to Dodgeball was because they are lazy and not because they had ulterior motives.

Irwin mentioned that Dodgeball helped to protect users. Dodgeball allowed users to ''block'' other users from ''seeing'' them, communicating with them, and interacting with them through the service. Dodgeball also allowed members to block a person who had been in their friend network from sending and receiving messages

without letting the other person know he or she had been blocked. Only 4 of the 21 informants had blocked anyone on Dodgeball. They blocked another user not because of stalking concerns, but because the friend had become annoying by sending too many messages through Dodgeball or they had had a falling out.

> Interviewer: How did you decide to block them?
> Yevette (San Francisco): One particular case, this person was checking in from work every single day and I felt like that's redundant. I'm kinda tired of getting that message every day, sometimes multiple times a day . . . . He would check in from places that weren't really, what's the word, really open for dropping by. Like he would check in from home or in Palo Alto or a place with his kids. That's not really of interest to me so I blocked him.

As Yevette mentioned, Dodgeball informants used blocking to manage awkward or annoying social situations rather than to protect themselves from stalking or lateral surveillance.

Deirdre, a Dodgeball informant from Minneapolis, had a slightly different perspective on the issue of lateral surveillance. She acknowledged that stalking *has* been a concern with new information technology, but suggested that perhaps such a concern is not the case anymore.

> I think [Dodgeball] is a really interesting subversion. For years and years, people have been like, "Oh don't tell anyone on the Internet about yourself. Don't tell 'em where you are." Well, this is something that is trying to broadcast exactly where you are. So it kind of subverts that notion that everyone is a sexual predator and that everyone online is evil. (Deirdre, Minneapolis)

Most of the Dodgeball informants were not concerned about lateral surveillance in the form of stalking, but expressed that they enjoyed using Dodgeball to learn where their friends hung out socially. They benefited from the mutual monitoring that Dodgeball allows. Nevertheless, this mutual monitoring could become asymmetrical (a) because not all people broadcasted personal information at the same rate and (b) because users did not always know when or if people access the information they broadcast over Dodgeball.

Self-surveillance

There were a number of technological features on Dodgeball that facilitated a form of self-surveillance through the ability to record one's behavior for viewing at a later time. For example, when users logged in to the Dodgeball Web site they could see a Google Map of all the places they had checked in over the last 24 hours, week, month, 6 months or a year. In addition to maps of their own check-ins, the Web site also listed the users' most recent check-ins on their profile webpages, as well as listing on the webpages of venues which Dodgeball members had recently checked in there.

Dodgeball also sent out a monthly e-mail digest to users of their check-ins as well as the friend's check-ins. As discussed above, Dodgeball users could also import RSS feeds of their check-ins to their blogs. Users could also import their check-ins into their calendar, such as Google Calendar or Outlook. Together, these mechanisms allowed Dodgeball users a way to record and catalog their own behavior for themselves.

A number of Dodgeball users indicated that they found great enjoyment in looking at the maps of their Dodgeball check-ins.

> You can see the Google maps and you can see all of the pins and you can definitely tell where there's (sic) clusters, which I also find interesting. Maybe [it's] because I analyze things, but I like having that too because you can see your patterns. (Enid, New York City)

The aggregation of individual Dodgeball behavior on maps allowed people to see patterns in their behavior that they might not have been aware of otherwise.

> I like the fact that it keeps track of where I've been and where I've checked in. And I can overlay that on a map along with where all my other friends checked in and just kind of get an idea of where's everybody been. (Dean, Chicago)

Like Dean, Irwin enjoyed the visualization of information through Dodgeball's mapping feature.

> I can go back and see a visual sort of pin chart of where I've been. [Dodgeball] really does give you sort of a different look. I always consider myself a very statistical outlier when it comes to these kinds of things. You know, I am an engineer. I love stats. I like looking at these things. I don't think anyone else was looking at Google maps of where they've been over the last year. I like, you know, overlaying maps of where I've checked in over the last year versus all the other friends I have on Dodgeball. Things like that. But again you're making something that's usually invisible, visible. (Irwin, Los Angeles)

The self-surveillance that Dodgeball facilitated allowed users like Irwin to see where he had been in ways that were previously much more difficult to do. Not only did Dodgeball keep an itemized list of his social outings, but also it created a visual representation of outings on the Google Map. By combining his map with the maps of his friends, he could visually compare and contrast social outings.

Other users felt Dodgeball allowed them the power to link their own behavior to databases in ways there were previously unavailable. Leonard was particularly thoughtful about how information was linked together.

> I feel like the layer of information currently exists in parallel to the physical object it's connected to. And I'm really interested in anything that can anchor the

> data layer onto the physical layer . . . . You know, like with Plazes or Dodgeball or whatever. And I just think it's so awesome that I can, you know, hyperlink reality to this database of places and people. I like being the bridge between the network and the real world. I like it. It's cool. (Leonard, Los Angeles)

Leonard was philosophical about his ability to link his Dodgeball information with other kinds of information like maps. He believed that Dodgeball helped him to link mediated and unmediated realities to create new mediaspaces. Leonard has both personal and professional interests in technology-enabled communities and new mediaspaces. He is an Online Content and Community Manager for a film production company in Los Angeles and is a very active blogger and reader of blogs. Leonard is, what Rogers (1995) would call an 'innovator.' Innovators are the first to adopt a particular innovation and are "active information-seekers about new ideas" (Rogers, 1995, p. 22). Leonard spends a lot of time thinking, reading, and writing about the relationships between online and offline communities and between databases and lived experiences. While Leonard was thoughtful and creative in his use and integration of Dodgeball, he is not representative of general Dodgeball users. Even among my informants, Leonard is atypically technologically sophisticated.

Other informants admitted that they liked using Dodgeball as a kind of social diary to record where they have been. By checking in at social outings, they had a log of their social calendar without having to plan everything out. For example, not only did Enid enjoy receiving the e-mail digests from Dodgeball, but also she suggested that this cataloging feature was part of why she used Dodgeball as often as she did.

> I like that Dodgeball sends you these digests every month, sort of like a log of everywhere you've checked in. So I also know in my head that it'll be stored somewhere. And I kinda like looking back on those things and seeing everywhere I was and the date and the times. That's another reason why I check in a lot . . . . I like that kind of stuff, like the social diary. It's almost that somebody's doing it for me. Like I'm passively, you know, adding all these things. (Enid, New York City)

While self-surveillance on Dodgeball was not entirely passive, Enid felt it could be used as a passive social diary that she could store on the Google server. Journals and diaries are an important way for people to connect the present to the past in their everyday lives (Rosenzweig & Thelen, 1998). The designers of Dodgeball recognized the social diary capabilities of Dodgeball and integrated the RSS feed and Google Calendar importation functionalities to encourage such use (Dennis Crowley, personal communication, May 11, 2006).

Dodgeball itself helped users to create a record of their behavior, but if paired with other collaborative technology, such as blogs or photo sharing sites, Dodgeball data could be richly linked to images and descriptions of social behavior. In some instances, Dodgeball members were so accustomed to socially cataloging their behavior on these sites or through check-ins that they expected their friends would do so as well. Dierdre

described a situation where differential use of these varying systems caused social friction among her friends.

> I get together with a smaller group and maybe we wouldn't check in. And the funny thing is that we're all on these other community websites, like Flickr . . . . And photos of us getting together would go up on Flickr and then people that are on our Dodgeball network would get upset. "How come you didn't check in? I saw pictures of you guys at that place and no one checked in. Are you trying to avoid me?" (Dierdre, Minneapolis)

Dierdre and her friends check in so often that when they did not, her other friend wondered if they purposefully chose not to do so because they were trying to avoid her. The various other collaborative technologies allowed her and her friends to catalog their night out so that other friends who were not there could find out despite not being in her Dodgeball network of friends. One of the main differences between "old-fashioned" journals or diaries and these online or mobile social blogs is the publicness of the journals. Friends, family members, employers, and even strangers could read or see the various social activities of Dodgeball members on the Dodgeball Web site or on blogs or community Web sites. As Dierdre demonstrates, there can be social repercussions even among friends from publicly sharing such information. Dierdre's situation also suggests that lateral surveillance on interactive technologies may in fact be much broader than just stalking. Expectations of continual information disclosure may arise among groups of friends and social friction or sanctions may occur when such expectations are violated.

Discussion

Privacy concerns among Dodgeball informants were minimal. Consistent with privacy research (Gandy, 1989; Stone, Gueutal, Gardner, & McClure, 1983), as long as people felt they were in control of their personal information they were unconcerned about their privacy. This is not a surprising finding because my informants were among the most active Dodgeball users in the country. Anyone who signed up for Dodgeball and had stopped using it due to privacy concerns or those who never even signed up for Dodgeball because of privacy concerns would not have entered into my study. Nevertheless, it is important to understand how highly active users do conceptualize and understand privacy when using mobile social networks because they are the early adopters who will help to shape normative practices and use of mobile social networks in the future.

Despite the lack of concern or privacy, there was evidence that mobile social networks can contribute to three kinds of surveillance. Once user information is relayed through a central server, it allows for corporate surveillance in that it creates a one-way system of monitoring behavior. Because mobile social networks, like other interactive services, are of some benefit to users, they willingly participate in the

surveillance of themselves by others. The voluntary or "participatory panopticon" (Whitaker, 1999) is so powerful because it is a consensual and de-centered surveillance. People willingly allow entities to monitor their behavior because such services provide a convenience for them. It is important to note that when I asked informants about privacy issues, no one brought up concerns about corporate or bureaucratic surveillance. While some scholars have argued that corporate surveillance can lead to discrimination and social control (Andrejevic, 2007; Gandy, 1993), this was not a salient concern for the participants in this study. While I am hesitant to over interpret this finding, it may suggest that such corporate surveillance is not an active concern to mobile media users. This seems to go against research that shows people are in fact concerned about companies monitoring their online behavior (e.g., Fox et al., 2000). That said, Pew found that when asked most Americans expressed concern about corporate tracking of their behavior, but their online behavior did not necessarily reflect this concern. "Despite Americans' high anxiety about being monitored online, only 10% of Internet users have set their browsers to reject cookies" (Fox et al., 2000, p. 3). The lack of saliency of corporate surveillance among the Dodgeball participants in this study may be related to this finding that behaviors do not reflect concerns about corporate surveillance. It may be that while some people are concerned about corporate surveillance, it is not a highly salient concern that influences their everyday online or mobile use.

Lateral surveillance is the monitoring of user behavior by other users and can also be achieved through mobile social networks, like Dodgeball. Users can monitor the behavior of other users. In fact, these systems rely on the monitoring of users by other users. Even if informants suggested that there was an asymmetrical monitoring of behavior among users, most informants were not generally concerned about lateral surveillance as it relates to stalking. Most felt they had control over their information and did not believe that other Dodgeball users would use their personal information against them.

The last kind of surveillance mobile social networks can contribute to is self-surveillance, where people record their own behavior to be reexamined at a later time. Some Dodgeball informants greatly enjoyed the self-surveillance that Dodgeball allowed through the visualization of check-in information on maps as well as the aggregation of socio-spatial network information presented on maps as friend check-ins. For some informants, such self-surveillance even motivated their use of the Dodgeball system. They checked in at many places because they wanted to be able to later see a map of their locations. The ability to record their behavior and see it later in a new way changed their future behavior of checking in to more venues.

It is also important to note that while Dodgeball facilitates all three kinds of surveillance, it does not do so evenly. The amount of information that Dodgeball and its partners have access to is far greater than the amount of information users have access to. Not only did the Dodgeball company have access to a greater breadth of information (i.e., information from all users across cities and friend networks), but it also had a greater depth of information (i.e., information which is not presented back

to users such as who responds to whose check-ins). In addition, each of the three kinds of surveillance evidenced in the Dodgeball case study contributes to a "digital enclosure" (Andrejevic, 2007). Despite people using the service to communicate with their friends, such usage of an interactive service generates information about behaviors, motivations, and desires that is valuable consumer data. Even if Dodgeball members use the service to better understand their own behaviors through a self-surveillance mechanism, the system could also be learning about their behaviors but on a much larger scale when aggregated with other types of consumer information.

Conclusion

New mediaspaces (Couldry & McCarthy, 2004) created by mobile and online social network services are not only spaces for communication, coordination, and interaction, but also monitored spaces of consumption and production. As people use these technologies to meet up, whether it be through an event organized through Facebook, an e-vite online, or a mobile network, like Dodgeball or foursquare, that shares real-time locations, users are not only telling their friends where they are or where they will be, but they are potentially telling this to marketers. This means that mobile and online social mediaspaces also become spaces of production.

> The de-differentiation of spaces of consumption and production achieved by new media serves as a form of spatial enclosure: a technology for enfolding previously unmonitored activities within the monitoring gaze of marketers. Spaces associated with leisure and domestic activities do become increasingly productive from a commercial point of view precisely because they can be more thoroughly monitored. (Andrejevic, 2004, p. 195)

Mobile and online social networks allow for the monitoring of behavior in ways that were previously unavailable to marketers. These spaces of sociality become sites of productivity. As people spend more time using these services, more of their personal information enters into the commercial gaze. Emerging interactive technologies are important sites through which to explore how information is collected and used, and the role of privacy and surveillance in this process.

The collection of personal information through mobile social networks is very much part of the surveillance society in which we live, but it is not inherently good or bad. Meyrowitz (2007, p. 20) argues that

> To say that the surveillance society we live in is neither clearly good nor bad, however, is not to say that it is neutral or has no impact on our lives. And the impact does not have to be in our constant awareness to be significant. Surveillance technologies are now so pervasive, yet so subtle—many occurring automatically as we engage in purchasing, driving, or walking down a street—that they may transform the texture of everyday life without most of us being aware of the change.

In this article, I have tried to identify and discuss how the collection and aggregation of socio spatial information of mobile social network users works in everyday practice. I have explored both micro and macro ways that such monitoring and surveillance manifests. I have also tried to ground a discussion of interactive technologies and surveillance in the everyday experience of Dodgeball users who overwhelmingly were not concerned about privacy and surveillance. This project is an early study of mobile social networks and thus provides a glimpse into future and long-term impacts of mobile social network usage. While the various kinds of surveillance that are at work on mobile social networks may seem and even currently be benign, it does open up possibilities for indirect or longer term ramifications and potential abuses of power.

This project specifically examined mobile social networks, but many of the same issues of surveillance and privacy may emerge regarding online social network sites. The cataloging of personal and location information that Dodgeball facilitates is not that dissimilar to news feeds or status updates on popular social network sites. These services both facilitate and rely on the mutual sharing of personal information. Future research should continue to explore everyday notions of surveillance, which users of these interactive technologies employ. One difference between mobile social networks and online social networks is the amount of information that users themselves have access to. Friends network online tends to be much larger than mobile social networks, thus there is more socio locational information available. This could lead to more advanced forms of lateral surveillance, but it could also simultaneously increase levels of social connectivity. For example, Lampe, Ellison, and Steinfield (2006) found that Facebook had a surveillance function whereby its members would browse the profiles of friends in order to ''track the action, beliefs and interests of the larger groups to which they belong'' (p. 167). This kind of surveillance may have positive social benefits to the individual and the group and should be further explored. While this fieldwork and interviews focused on the issue of privacy for Dodgeball users, future research should also more explicitly probe how users of social media think their personal information is being used. Reframing the interview in such a way could shed light on additional tacit normative expectations of information management and surveillance.

The collection and aggregation of information through new communication technologies may bring about many important opportunities for social connectivity and awareness, but also opens up room for potential abuse from either corporate and bureaucratic entities or socially maladjusted individuals. Information technology is not inherently a good or bad force in society but it does impact our lives in a variety of ways. This study was an attempt to explore some of the ways that different entities can use the information collected through mobile social networks, thus demonstrating a complexity of understanding that such technology warrants in our everyday lives.

Acknowledgment

The author thanks the reviewers for their insightful suggestions and comments.

Notes

1 This understanding of self-surveillance is similar to Vas and Bruno's (2003) discussion of self-surveillance, as "individuals' attention to their actions and thoughts when constituting themselves as subjects of their conduct." (p. 273). In both situations the ability to observe one's own behavior beyond one's personal experience calls attention to particular aspects of the behavior that one may not even be aware of. Both definitions are extensions understanding self-surveillances as self-monitoring which result from the real or potential observation by another who in a position to control (Foucault, 1977).
2 All Dodgeball informants are identified by pseudonym only.

References

Anderson, J. Q., & Rainie, L. (2008). *The future of the Internet III.* Washington, DC: Pew Internet & American Life Project.

Andrejevic, M. (2004). The webcam subculture and the digital enclosure. In N. Couldry & A. McCarthy (Eds.), *MediaSpace: Place, scale and culture in a media age* (pp. 193–208). London: Routledge.

Andrejevic, M. (2006). The discipline of watching: Detection, risk, and lateral surveillance. *Critical Studies in Media Communication*, **23**, 391–407.

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era.* Lawrence: University Press of Kansas.

boyd, d. m. (2004). Friendster and publicly articulated social networking. *Proceedings of the ACM Conference on Computer Human Interaction (CHI2004), USA*, 1279–1282.

boyd, d. m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer Mediated Communication*, **13**(1): 210–230.

Couldry, N., & McCarthy, A. (Eds.). (2004). *MediaSpace: Place, scale and culture in a media age.* London: Routledge.

Crowley, D. (2007). Me & Alex quit Google. (Dodgeball forever). Retrieved from http://www.flickr.com/photos/dpstyles/460987802/.

CTIA. (2011). *Semi-annual wireless industry survey: Annualized wireless industry survey results—Year-End 2010 Top-Line Survey Results.* Washington, DC: CTIA— The Wireless Association.

Dodgeball. (2005). Dodgeball's privacy statement. Retrieved from www.Dodgeball.com/privacy.

Ellison, N., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": Exploring the relationship between college students' use of online social networks and social capital. *Journal of Computer-Mediated Communication*, **12**(4), 1143–1168.

Elmer, G. (1997). Spaces of surveillance: Indexicality and solicitation on the internet. *Critical Studies in Mass Communication*, **14**, 182–191.

Elmer, G. (2003). A diagram of panoptic surveillance. *New Media & Society*, **5**, 231–247.

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). New York: Pantheon Books.

Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., & Carter, C. (2000). *Trust and privacy online: Why Americans want to rewrite the rules.* Washington, DC: Pew Internet & American Life Project.

Gandy, O. H., Jr. (1989). The surveillance society: Information technology and bureaucratic social control. *Journal of Communication*, **39**(3), 61–76.
Gandy, O. H., Jr. (1993). *The panoptic sort: A political economy of personal information.* Boulder, CO: Westview Press.
Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research.* New York: Aldine de Gruyter.
Google. (2009, June 15). Mobile privacy policy. Mountain View, CA. Retrieved from http://m.google.com/static/en/privacy.html.
Humphreys, L. (2007). Mobile social networks and social practice: A case study of Dodgeball. *Journal of Computer-Mediated Communication*, **13**(1): 341–360.
Kay, P. (1978). Policy issues in interactive cable television. *Journal of Communication*, **28**(2), 202–208.
Lampe, C., Ellison, N., & Steinfield, C. (2006). A Face(book) in the crowd: Social searching vs. social browsing. *Proceedings of the ACM Conference on Computer Supported Collaborative Work (CSCW2006), USA*, 167–170.
Lofland, J., Snow, D. A., Anderson, L., & Lofland, L. H. (2006). *Analyzing social settings: A guide to qualitative observation and analysis* (4th ed.). Belmont, CA: Wadsworth/Thomson Learning.
Lyon, D. (2001). *Surveillance society: Monitoring in everyday life.* Buckingham: Open University Press.
McFarlane, L., & Bocij, P. (2003). An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First Monday*, **8**(9), article 5. Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1076/996
McLuhan, M., & Powers, B. (1980). Electronic banking and the death of privacy. *Journal of Communication*, **31**(1), 164–169.
Meyrowitz, J. (2007). *Watching us being watched: State, corporate, and citizen surveillance.* Paper presented at the symposium "The End of Television? Its Impact on the World (So Far)." Annenberg School for Communication, University of Pennsylvania, Philadelphia.
Poster, M. (1990). *The mode of information: Poststructuralism and social construct.* Chicago: University of Chicago Press.
Rogers, E. (1995). *Diffusion of innovations* (4th ed.). New York: Free Press.
Rosenzweig, R., & Thelen, D. (1998). *The presence of the past: Popular uses of history in American life.* New York: Columbia University Press.
Shirky, C. (2005, May 11). Google acquires Dodgeball. Retrieved from http://many.corante.com/archives/2005/05/11/google_acquires_dodgeball.php.
Stone, E., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, **68**, 459–468.
Vas, P., & Bruno, F. (2003). Types of self-surveillance: From abnormality to individuals 'at risk'. *Surveillance and Society*, **1**, 272–291.
Vidmar, N., & Flaherty, D. H. (1985). Concern for personal privacy in an electronic age. *Journal of Communication*, **35**(2), 91–93.
Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, **59**, 431–453.
Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality.* New York: New Press.