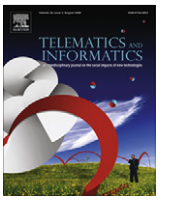
Telematics and Informatics 30 (2013) 11–21

Contents lists available at SciVerse ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele



Sousveillance: Communities of resistance to the surveillance environment

Jan Fernback *

Department of Broadcasting, Telecommunications and Mass Media, Temple University, 2020 N. 13th Street, Annenberg 205, Philadelphia, PA 19122-6080, United States

ARTICLE INFO

Article history:
Available online 21 March 2012

Keywords:
Facebook
Surveillance
Sousveillance
Privacy

ABSTRACT

Facebook is often invoked in popular discourse as a device for the potential exploitation of individual privacy. Facebook users invite surveillance, and personal information revealed by Facebook users is compiled into aggregated databases of linked information, preferences, and behaviors. In the interest of the ideals of individual empowerment, cultural integrity, social responsibility and equality, social networking communities are forming to interrogate networked surveillance. This article examines those communities of resistance in the form of "sousveillance" tactics that have emerged as a backlash to the surveilled environment. Sousveillance is "watching from below," a form of inverse surveillance in which people monitor the surveillors. Examples include citizen video, watchdog web sites, or the monitoring of authorities (corporations, military, government). Sousveillance embraces the idea of transparency as an antidote to concentrated power in the hands of surveillors. Sousveillance is used in Facebook itself to expose the data gathered by Facebook to the larger networked population. The surveillance sector's responses to citizen resistance may ultimately alter the power dynamic between the watchers and the watched. Implications for this power dynamic are discussed through an exploration of Facebook sousveillance communities of resistance and how they are sustained in an effort to contribute to the larger examination of hegemonic practices in the global information society.

1. Introduction

Facebook is often invoked in popular discourse as a device for the potential exploitation of individual privacy, and much is written about Facebook as a surveilled realm (Hodgkinson, 2008; Sanchez, 2009; Melber, 2008). Online social networks enable environments of both watching and being watched. Because Facebook encourages social intimacy through information sharing, users invite surveillance by agreeing to the service's terms and conditions and by crafting profiles, photo albums, news feeds, and ultimately, online identities. Simultaneously, Facebook's data mining metrics compile dossiers of personally identifiable information about users. Personal information revealed by Facebook users is compiled into databases of linked information, preferences, behaviors, and so forth. Can Facebook users mitigate the potential negative consequences of information surveillance if the collection of information is managed and controlled rather than blocked altogether? In the interest of imagining an "informed knowledge society" responsive to the ideals of individual empowerment, cultural integrity, social responsibility and equality, social networking service (SNS) communities are forming to interrogate networked surveillance. This paper examines those communities of resistance in the form of "sousveillance" tactics that have emerged as a backlash

* Tel.: +1 215 204 3041; fax: +1 215 204 5402.
E-mail address: fernback@temple.edu

0736-5853/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.tele.2012.03.003

to the surveilled environment. Using a critical orientation, this research comments on the fluid power dynamic between individuals and institutions fortified by the technological revolution.

2. Critiques of Facebook as a surveillance mechanism

Surveillance is the practice of rigorous monitoring, sometimes openly and sometimes illicitly, of human data for the purposes of control. Facebook, like other online services such as Google, has been faulted for the systematic surveillance of its users in critiques that usually focus on violations of user privacy. Facebook's data collection operations involve a number of applications and algorithms, including general application programming interfaces (APIs), that reveal connections between various applications, operating systems, libraries and so forth. Examples might include geotagging embedded in photos posted to a user's profile; clicking the "like" button; or sharing information through Facebook on sites such as Flickr. While Facebook's exact metrics are proprietary information, the site provides various constituencies (developers, advertisers and marketers) with clues as to how specific data mining techniques operate. Facebook explains to advertisers how/what to target with this text:

> Any number of targeting filters can be set for an ad. You can choose to use the default targeting which are people located in your country over the age of 18. Or you can refine that targeting to include other locations, demographics, likes and interests and/or connections. For instance, you can target women in the United Kingdom who are between 18 and 35 years of age and are interested in mechanical engineering (http://www.facebook.com/adsmarketing/index.php?sk= targeting_filters).

In order to make sense of the data collected by these devices and metrics, models are created that associate information into recognizable patterns such as connecting demographic data with consumer behavior. This modeling is achieved through computer algorithms, graphical interfaces, and network mapping. Although Facebook (and other sites) overtly collect personally identifiable information, critiques of Facebook's techniques for gathering data have been frequent and boisterous.

In an analysis of the various privacy issues that have beset Facebook, Eldon (2010) finds that Facebook's attempts to make more user data available to marketers or developers has resulted in user protests, policy changes, legal actions, and investigations. According to Eldon (2010), users demonstrate confusion with regard to Facebook's numerous and confounding changes to its privacy policies. One of the company's most criticized changes involved the use of Beacon, a social advertising mechanism launched in 2007, which tracked purchasing activity online and shared it across a user's network without permission. Thus, a user's activities online became what Melber (2008, p. 22) referred to as "turning private commerce into public endorsements." Moveon.org created a Facebook group to demand that Beacon be recast as an "opt-in" program, Facebook suffered public cries of foul, some advertisers backpedaled, and some lawsuits were initiated (Eldon, 2010; Melber, 2008).

Another strongly criticized change to Facebook's privacy policies involved the use of the News Feed and the Mini-Feed, unveiled in 2006. The News Feed altered the original look of a member's site, appearing on users' home pages and displaying the activities (including wall conversations, birthday notifications, events, etc.) of the user and user's network of friends. The Mini-Feed provided a log of the user's activities appearing on the user's profile page. While the Mini-Feed could be manipulated to keep information invisible, the News Feed had no customizable settings. Criticism arose surrounding the ability of anyone in a member's network to be able to view user activities, thus denying a user true control over activity information (Sanchez, 2009). The group *Students Against Facebook News Feed* appeared to protest the nature of the changes that negated users' capacity to portray themselves in accordance with their own preferences (Sanchez, 2009). Facebook responded by altering privacy settings to control access to status updates so that everyone, friends of friends, or friends only could view the News Feed.

More recent controversies erupted after Facebook required users to transition to new privacy settings that confused some users by prompting them to make information more public instead of more private (Eldon, 2010). The transition tool required users to alter their profiles so that personal interests were recast as public information. This information includes a member's home town, sexual orientation, birthday, biography, interests, political and religious views, education and employment, lists of friends and relatives, relationship status, photo albums, posts to friends' walls, comments on those posts, and the ability of others to view those posts. A user wishing to opt out of this requirement had to permanently delete the information or re-enter it. Concerns centered around the fact that previously private information was involuntarily altered to become public (Eldon, 2010). Privacy concerns were raised again after Facebook developed the Open Graph API, which permits developers access to user data based on what users have "liked" on Facebook. Along with social plugins which allow users to share brands or sites they "like" in news feeds and creates widgets so sites can customize themselves to those users and friends (Eldon, 2010), Open Graph integrates Facebook more seamlessly with third party applications and sites. Open Graph permits developers to publish to users' data streams. The "like" function gathers data on users' online activities and, with updates to Facebook's privacy policy, stores the data for an indeterminate time (Warren, 2010; Eldon, 2010). As a result, Warren (2010) claims that "public no longer means "public on Facebook," it means "public in the Facebook ecosystem." Clearly, responsibility for privacy is borne more by the user than by Facebook. The majority of users, however, have little understanding that "restricting access to their data does not sufficiently address the risks resulting from the amount, quality and persistence of the data they provide" (Debatin et al., 2009, p. 103). Warren (2010) adds, "users need to assume