Studies in Communication Sciences 15 (2015) 221–228

Contents lists available at ScienceDirect

Studies in Communication Sciences

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

Electronic surveillance on Social Networking Sites. A critical case study of the usage of SNSs by students in Sassari, Italy

Massimo Ragnedda*

Department of Media, Communication and Design, Northumbria University, Newcastle upon Tyne, United Kingdom

ARTICLE INFO

Article history:
Received 14 June 2014
Accepted 21 May 2015

Keywords:
Dataveillance
Surveillance
Facebook surveillance
Social Networking Sites
Surveillance
Privacy

ABSTRACT

This paper presents some theoretical considerations arising from empirical research conducted on students from the University of Sassari, Italy (*n*: 1047). Students have little knowledge of the laws in Italy that regulate surveillance, and they underestimate the extent of dataveillance and e-surveillance. Some interesting findings include: only 30.9% of respondents were aware that Facebook is always allowed to collect and store data on their information behaviour (meaning that around 70% did not know) and only 23.9% knew that Facebook is allowed to reuse and resell personal data (so more than three out of four students did not know). However, half of respondents agreed or strongly agreed that private firms have strong interests in gathering the personal data of Internet users. Furthermore, 58.5% knew that the advertising clients of Facebook are allowed to gather data on users' information consumption. These data are particularly interesting because they have been collected and analyzed before the PRISM-gate scandal erupted and became popular. In considering these data within a wider framework of data surveillance, this paper also explores the connections between such attitudes and knowledge of and attitudes towards surveillance by social networking sites.

1. Introduction

There is a need to investigate, study and characterize the surveillance and security of online social media from various perspectives: cultural, computational, psychological and sociological. Such surveillance practices compromise both social relations and the political economy of personal information (Cohen, 2008).

The extensive use of social networking sites (SNSs) offers new opportunities for interaction and they have become integrated into modern-day social interactions, being widely used as a primary medium for communication and networking, especially among young persons (Cecez-Kecmanovic, Ariadne, & Kenna, 2010). Thanks to these SNSs, millions of individuals create online profiles and share personal information within their networks of friends (Brandtzæg & Marika, 2010), and increasingly with unknown strangers, corporations and even governments. First of all, it bears noting that SNSs are dominating online activities today (Boyd & Ellison, 2007; Lenhart & Madden, 2007), and the large interest in SNSs is reflected in rising amount of academic studies of SNSs. Danah Boyd has gathered a collection of research about SNS which lists more than 650 among research papers, books, and research reports published in the years 2003–2014.

As of October 2014, Facebook has accumulated, from around the world, more than a billion users (1,310,000,000) and half of them (48%) log on in any given day. In Italy, the number of users is more than 20 million. This makes it 11th in the ranking of all Facebook statistics by country, with a penetration of the total population around 37% and the online population some 72%. In reflecting the popularity of Facebook, the paper will present and discuss some theoretical views deriving from empirical research conducted on the students from the University of Sassari, Italy (*n* = 1047). The research attempted to point out how unaware most students are in relation to online surveillance, and how unquestioning they are about e-surveillance by the state and private firms. The research therefore attempts to understand:

- How knowledgeable are students about surveillance in society?
- How aware are students about potential surveillance by states and/or corporations?
- Are students concerned enough about the security of personal data?

* Tel.: +44 01912437444.
E-mail address: ragnedda@gmail.com

http://dx.doi.org/10.1016/j.scoms.2015.05.001

Many studies have been carried out on the topic of awareness of citizens/consumers about corporate surveillance or about privacy perception and surveillance awareness (Ragnedda, 2013; Boyd & Hargittai, 2010; Hoofnagle & King, 2008; McRobb & Bernd, 2007; Milne, Rohm, & Bahl, 2004; Turow, Feldman, & Meltzer, 2005). More specifically, about students' perception of online privacy some research has been conducted in different countries across Europe, such as Austria (Fuchs, 2009a) and England (Oxford Internet Institute) or in the USA (Lewis, Kaufman, & Christakis, 2008). However, the research questions leading this work emerge from a gap in the literature review that I would like to fulfil. Indeed, no research has been conducted in Italy so far. This is the reason why the present research is based on data collected at a university in Italy.

Firstly, some theoretical background that has guided this research project will be given. Then, the research methodology will be explained and the results of the study presented and discussed. Finally, some conclusions will be drawn.

2. Theoretical background

The increased visibility of personal information through SNSs, and more specifically Facebook, makes this a crucial topic for surveillance studies. The SNSs raise new privacy concerns (Bilton, 2010; Fletcher, 2010; Fogel & Nehmad, 2008) because users conceal and reveal 'private' information, blurring boundaries between private and public life (Marwick & Boyd, 2011).

In fact, massive stores of personal data, held on ordinary people across Europe, are now vital to both public services and private business purposes. Borrowing the well-known concept of the iron cage formulated by Weber (1905) and adapted to the new digital era, we can argue that the new cages are no longer iron but electronic. Weber viewed the iron cage of rationality as a symbol of the social pressure that traps individuals in a system based merely on rational calculation, efficiency, and more importantly control. The new 'electronic cages' are more sophisticated and comprehensive, being able to produce in real time a complete e-profile of citizens and customers' preferences, enhancing social pressure and control. Techniques for processing personal information (Humphreys, 2011), which might have raised eyebrows in the world before September 11, suddenly seemed indispensable both by the public authority and public opinion. Manuel Castells considers Internet surveillance to be a technology of control (2001: 171), one that allows 'tracking of communication flows [. . .]. Then, by persuasion or coercion, governments, companies, or courts may obtain from the Internet service provider the identity of the potential culprit by using identification technologies, or simply by looking up their listings when the information is available' (Castells, 2001: 172). New information technologies have introduced a highly automated and much cheaper systematic observation of data on people by users, a well-known process as 'dataveillance' or 'actuarial surveillance' (Clarke, 1988; Phillips, 2010). ICTs advance the intensification and the extension of surveillance and thus pose problems for privacy (Musiani, 2010). Indeed, privacy is one of the rights under constant pressure through scientific and technological progress. As Boyd rightly pointed out, 'privacy is not an inalienable right–it is a privilege that must be protected socially and structurally in order to exist' (2008). The point is to critically understand whether or not this right is 'something that society wishes to support' (Boyd, 2008). The right to be left alone, to quote the well-known idea of privacy formulated by Warren and Brandeis (1890), must be revisited in the time of SNSs. This era seems to be characterized by what Barnes (2006) has defined as the 'privacy paradox', namely the idea that 'adults are concerned about invasion of privacy, while teens freely give up personal information. . . (and) this occurs because often teens are not aware of the public nature of the Internet'. However, several and more recent research studies have shown that users are worried about their privacy online, while they do not apply these worries to usage behaviour (Blank, Bolsover, & Dubois, 2014; Boyd & Hargittai, 2010; Debatin, Lovejoy, Horn, & Hughes, 2009; Taddicken, 2014; Tufekci, 2014). One of the goals of this research is to analyze the 'levels of self-disclosure', underlining what kind of personal data users tend to disclose online. A huge amount of data can now be collected, tabulated and cross-referenced much faster and more accurately than with old paper files before 1989, building a 'new electronic cage' inside which the individual is placed, largely on the basis of his e-profile and data matching. Through this new digital technology, 'surveillance becomes more ubiquitous, automatic, anonymous, decentralized, and self-reinforcing' (Parenti, 2003: 78). David Lyon has characterized surveillance as 'any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered' (2001: 2), and Gary T. Marx defines the new surveillance as 'the use of technical means to extract or create personal data. This may be taken from individuals or contexts' (2002: 12). Surveillance remains a central organizing practice and it is needed to create a safe and secure society in terms of extremism and criminality. At the same time, it is increasingly deployed to track customer behaviour, both offline and online, to deliver personalized services that offer more targeted information and to identify new business opportunities. Yet at the same time it raises fundamental questions about privacy, security and civil liberties. Lyon (2001: 3) notes this Janus-faced nature of surveillance, which 'both enables and constrains, involves care and control'. This neutral notion of surveillance is used, among others, by Giddens, who argues that it enables modern organizations to simplify human existence. He sees the 'surveillance as the mobilizing of administrative power – through the storage and control of information – is the primary means of the concentration of authoritative resources involved in the formation of the nation-state' (Giddens, 1995: 181). In some ways this is true, since gathering and processing personal data in searchable databases drives administrative efficiency. However, the idea of surveillance as applied to this research is more critical and could be seen as the collection and usage of data on individuals or groups so that control and discipline of individual behaviour can be potentially coerced or exercised. Indeed, as this paper suggests, users see state surveillance and corporate surveillance differently, and this research takes this into account.

Furthermore, surveillance is now enhanced by the process of digitalization that made possible 'lateral surveillance' (Andrejevic, 2005), intended as the peer-to-peer monitoring that amplifies the top–down monitoring, 'participatory surveillance' (Albrechtslund, 2008), intended as the fact that we are performing surveillance on ourselves revealing exhaustive personal information on public websites and allowing corporations and governments to see, analyze, and store them; or 'social surveillance' (Tokunaga, 2011), intended as the activities to survey content created by others and observing one's own content through other people's eyes. With the Internet, state surveillance and private-commercial surveillance 'foster asymmetrical and undemocratic power relations. Political and economic elites collect information that facilitates social Taylorism rather than fostering more democratic forms of shared control and participation' (Andrejevic, 2007: 257). Andrejevic sees the Internet as a digital enclosure (2004, 2007), one in which interactive technologies generate 'feedback about the transactions themselves', and he further notes that this feedback 'becomes the property of private companies' (Andrejevic, 2007: 3). Currently, it might be observed that both governments and the private sector potentially have both a larger quantity and better quality of detailed information about citizens than the KGB or Stasi used to have on their own citizens during their regimes. However, users seem to be more concerned about interpersonal electronic surveillance (IES)