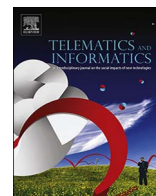




Contents lists available at ScienceDirect

Telematics and Informatics

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

Track me, track me not: Support and consent to state and private sector surveillance

Nili Steinfeld

Ariel University, Ariel, Israel

ARTICLE INFO

Keywords:

Privacy
Surveillance
Consent
Experiment
Security

ABSTRACT

The current study examines consent to surveillance and identifies links between support for state surveillance and consent to surveillance by private entities. Contrary to a tendency in academic literature and public debates to consider private and state surveillance as a single phenomenon in terms of methods, magnitude, and practice, findings show that individuals distinguish between these two types of surveillance when it comes to compliance and consent. Support for state surveillance is much more widespread and does not correlate with consent to private sector surveillance. Furthermore, support and consent to surveillance are rather nuanced, with different factors predicting different types of surveillance, according to the justifications and contexts of surveillance methods: Private sector surveillance is predicted by the compensation offered to subjects, factors related to behavior in online social networks and age. With regard to state surveillance- support varies between surveillance as part of the war against terrorism, which is most common and predicted by political trust and support for other types of state surveillance, surveillance for security reasons which is predicted by age, political interest, political orientation and support for anti-terror surveillance, and surveillance in general- which is least common and predicted by religiosity, level of privacy settings in SNS, political trust and anti-terror surveillance.

1. Introduction

In today's modern societies, diverse actors, including governmental and private sector entities, engage in surveillance- primarily the collection, storage, and analysis of personal information.

State and private sector surveillance differ in scope, authority, aims and motivations: In the case of the private sector, data collection is said to be used to improve service, or to match advertising to our interests. In the state's case, surveillance is justified as a necessary mean to ensure the security of citizens, fight terrorism, maintain public order, or improve governance. One important aim of surveillance systems in modern welfare states is to distinguish between citizens and foreigners in order to ensure that all entitled citizens receive public services (Broeders, 2009).

Nonetheless, scholars often address surveillance as a single category. Staples groups together state and private surveillance by acknowledging that no matter what the motivation is, the intent of all sorts of surveillance is to modify actions and behaviors- of consumers, employees, citizens or foreigners (Staples, 2014). State and private agencies gradually rely on very personal information posted voluntarily by users on the Internet (Warwick, 2014), and in recent years, e-government services gradually appropriate commercial methods for personalizing services to users or target groups (Krishnaraju et al., 2016; Osman et al., 2014). Edward Snowden's revelations in 2013 affirmed just how deep the cooperation between corporations and the state is when it comes to sharing

E-mail address: nilisteinfeld@gmail.com.

<http://dx.doi.org/10.1016/j.tele.2017.07.012>

Received 24 May 2017; Received in revised form 3 July 2017; Accepted 20 July 2017
0736-5853/ © 2017 Elsevier Ltd. All rights reserved.

information about individuals (Lyon, 2014), making a case for addressing state and private sector surveillance as a single phenomenon.

Do users share the view of state and private surveillance being one single phenomenon, and is this view reflected in their compliance with surveillance? This study asks whether commonalities between state and private sector surveillance are manifested in individuals' perceptions and support of surveillance. The aim of the study is to characterize supporters of government surveillance and consenters to private sector surveillance, and ask whether support for state surveillance correlates with consent to private sector surveillance. Such correlation, if exists, may have far reaching implications on citizens compliance with state surveillance. Finding similarities, or rather pointing at differences between consenters and supporters of commercial and state surveillance may help characterizing participants of different types of surveillance and their motivations.

2. Literature review

2.1. Defining surveillance

Privacy literature, including surveillance studies, is highly diverse and often inconsistent, and its greatest challenge is the very definition of its terminology. The difficulty in defining the philosophical and social justifications of the right to privacy is further compounded in the case of online privacy, as social, technological and legal developments continually influence and shape the debate over the definitions and boundaries of privacy (Hallinan et al., 2012; Rainie and Anderson, 2014).

The definition of surveillance is also ambiguous. The most familiar symbol of modern surveillance is Samuel Bentham's Panopticon, popularized in the twentieth century by Foucault (1995). It is a circular building, occupied by divided cells that ensure the secluded confinement of the tenants. The inspector's lodge is located at the center, making it possible to view all parts of the cells from the lodge, while tenants are unable to know when they are being observed (Bentham, 1791). The Panopticon serves a system of domination and discipline, eliminating a need for chains or locks, inducing in prisoners a consciousness of constant surveillance, knowing that in any given moment they are potentially being watched by the authorities (Allmer, 2011; Broeders, 2009; Schreiber, 2014). However, scholars diverge on whether the Panopticon is a suitable metaphor for the discussion on modern surveillance. Some say that the Panopticon image no longer represents surveillance systems, which are more data-oriented, decentralized and physically unbound, and are often desired or initiated by the individuals themselves (Allmer, 2011; Broeders, 2009; Lyon, 2003) for example, when citizens voluntarily participate in national surveys, interact with government officials and institutes via social network sites or government websites, install and deploy surveillance technologies etc.

Some definitions of modern surveillance offer a narrower conception, focused on data, primarily collection and analysis of information about members of a society (Allmer, 2011; Giddens, 1987; Lyon, 2001). In his taxonomy of privacy violations, Solove (2008) classifies surveillance strictly under information collection, further restricting its scope.

Surveillance is also conceptualized in terms of control. Deleuze (as cited in Best, 2010) uses the term "control society" to describe a further shift from Foucault's disciplinary society, reflecting the increasing self-discipline that characterizes modern societies, in which individuals voluntarily enter the system of control. Lyon (2001) adds another dimension to the control paradigm by describing the purpose of surveillance as 'influencing or managing those whose data has been garnered' (p. 2). Many references to surveillance stress its use for inclusion and exclusion of different groups in society, which is euphemistically referred to as "social sorting" (Best, 2010; Broeders, 2009; Lyon, 2003).

Developments in digital technologies drastically influence surveillance in several respects. Technological developments enable the monitoring of individuals with no physical limitations or presence. As a result, digital surveillance systems are everywhere, and they dramatically enhance the scope, reach and intensity of surveillance. The ability to integrate and cross-reference sources from various databases enhances the effectiveness of surveillance, or dataveillance, systems (Best, 2010; Broeders, 2009; Graham and Wood, 2003). Algorithmic surveillance further increases surveillance efficiencies by automating multiple processes, including the classification of persons or groups, comparison, prediction or responses to predefined conditions (Graham and Wood, 2003).

Surveillance can have positive as well as negative effects, and it is sometimes considered crucial for the safety of citizens and for public order (Lyon, 2001, 2003). Algorithmic surveillance systems arguably improve conventional systems by reducing the potential for corruption and discrimination, but they are also criticized for their automated "blind" operation that eliminates human involvement and assessment. Furthermore, seemingly "objective" software is argued to reflect social norms, interests and power dynamics, and thus increase digital divides (Graham and Wood, 2003). However, surveillance systems are neither "good" nor "bad" in themselves: Their effects on individuals and society are the result of the ways in which they are used, which are determined by their operators, and thus are subject to (intentional or unintentional) political and social biases (Graham and Wood, 2003; Lyon, 2003).

2.2. State and private (economic) surveillance

Writings about the historical roots of modern surveillance link it to the rise of the nation state, and describe surveillance as an instrument of state power (Barnard-Wills, 2012; Broeders, 2009; Foucault, 1995; Graham and Wood, 2003). But surveillance studies nowadays tend to describe it as an everyday practice that occurs everywhere, and involves everyone (Lyon, 2003). Surveillance is sometimes discussed as an individual practice, conducted by any person, creating in the target of surveillance a consciousness of being constantly observed (Schreiber, 2014). The increasing privatization of public services and the economic motives of commercial bodies to assess and classify users based on profitability, have resulted in the penetration of surveillance practice into the commercial sphere, which is referred to as economic surveillance: The monitoring of consumers or employees, when personal data constitute

Download English Version:

<https://daneshyari.com/en/article/6889884>

Download Persian Version:

<https://daneshyari.com/article/6889884>

[Daneshyari.com](https://daneshyari.com)