Government Information Quarterly 32 (2015) 129–141

Contents lists available at ScienceDirect

Government Information Quarterly

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

# Public opinion on National Security Agency surveillance programs: A multi-method approach

Christopher G. Reddick [a,*], Akemi Takeoka Chatfield [b], Patricia A. Jaramillo [a]

[a] Department of Public Administration, The University of Texas at San Antonio, 501 W. César E. Chávez Boulevard, San Antonio, TX 78207, USA
[b] School of Information Systems and Technology, Faculty of Engineering and Information Sciences, University of Wollongong, Wollongong, NSW 2522, Australia

ARTICLE INFO

Available online 17 March 2015

*Keywords:*
Government surveillance
Citizen-centric e-governance
Twitter
E-government
Public opinion
Logistic regression analysis
Critical discourse analysis

ABSTRACT

This paper examines public opinion on National Security Agency (NSA) mass surveillance programs of Americans. A new theory, developed and tested in this paper, explicates the effect of political efficacy on creating greater citizen-centric e-governance. Its propositions state that the higher citizens' perceived self-efficacy in political knowledge and the higher citizens' perceived fairness of government procedures and outcomes, the more engaged citizens would be in using technology for better governance and the more vocal in their views on NSA surveillance programs. This paper adopts a multi-method research approach to examine citizens' approval/disapproval of NSA surveillance programs: (1) critical discourse analysis of tweets exchanged among citizens and interest groups in Twittersphere and (2) logistic regression analysis of survey data collected from a random sample public opinion poll of Americans. The findings of both analyses provide evidence that citizens hold strong views toward NSA surveillance programs. These findings indicate that government needs to be more efficacious in communicating about surveillance programs more transparently to garner greater citizens' approval for its surveillance programs. The findings also provide preliminary evidence for good explanatory power of the theory of citizen-centric e-governance. The theory explains effectively the relationship between government practicing greater political efficacious behavior and citizens engaging in more citizen-centric e-governance in governing government surveillance programs for a better balance between security and privacy.



## 1. Introduction

In an era of digital government, public sector organizations are increasingly using data to improve their performance, provide greater citizen engagement, and cultivate levels of collaboration and transparency. This recent strategic thinking has led public sector organizations to make large-scale investments in surveillance technologies for collecting business intelligence and generating what has been labeled "big data." In the U.S., the Obama administration has made a move toward open data and data-driven public policy and public administration practices. National level government agencies across the globe, but most notably National Security Agency (NSA), have also increased their investments in technology-dependent national surveillance programs.

This paper explores, through a multi-method approach, public opinion on NSA surveillance programs. A review of extant literature finds that the views of citizens on government surveillance have not been thoroughly investigated. There is a clear lack of systematic understanding of citizens' views on government surveillance. In consequence, the literature has paid little attention to the potential roles played by net-savvy citizens in democratically governing government surveillance — not only more actively monitoring public administration of intelligence data collection, but also more proactively voicing their views on effective use of intelligence data for the good of the nation: government legitimacy, transparency, accountability and a better balance between national security and civil liberties.

Governments now have the potential to analyze massive amounts of collected data. The issue is that public policy has not kept up with advances in information technology (IT). There is much research that explores the issues associated (both legally and administratively) with a surveillance society, but citizens' views have been neither really fully understood nor gainfully reflected into making more balanced policy decisions. Therefore, this paper addresses the following research question: Are citizens, who are more engaged in government and policy, essentially having greater political efficacy, more likely to hold different views on the NSA surveillance program than those less engaged? In addressing the research question, this paper has integrated the literature and developed a theory of citizen-centric e-governance, which focuses on democratic governance roles of citizens in government surveillance. It has also used a multi-method approach of analysis of a public opinion

* Corresponding author.
*E-mail addresses:* chris.reddick@utsa.edu (C.G. Reddick), akemi@uow.edu.au (A.T. Chatfield), patricia.jaramillo@utsa.edu (P.A. Jaramillo).

http://dx.doi.org/10.1016/j.giq.2015.01.003
0740-624X/

survey and Twitter-enabled public discourse via #nsa to better understand citizens.

In this paper, we examine the theoretical relationship between political efficacy and citizen-centric e-governance. Here political efficacy examines citizens and their faith and trust in government in response to their perceived fairness of political procedures and outcomes, and from this it can explain how citizens can influence public affairs and policy. Citizen-centric e-governance is the focus of IT on enhancing the ability of citizens to democratically engage with political discourse and decision-making and hence influence meaningful change in public policy. Therefore, this paper aims to contribute to the literature by theoretically and empirically understanding the views of citizens as a key to moving toward greater citizen-centric e-governance in balancing the inherent tradeoffs between national security and civil liberties.

The organization of our paper is as follows. Second 2 examines the literature on government surveillance. In section 3 we then focus on the research on NSA surveillance program. Section 4 examines political efficacy and citizen-centric e-governance, which is our framework that is tested. Section 5 outlines the multi-method research methods of the paper and explores the research findings. Section 6 provides a discussion of the most significant findings and discusses the importance of this research, and efforts to move forward in this research domain are examined.

## 2. Government surveillance

Internet technologies provide more of an opportunity for governments for unobtrusive surveillance of information related to personal interests (Dinev, Hart, & Mullen, 2008). Brown and Korff (2009) argue that new surveillance technologies have the ability to monitor, screen, and analyze billions of telephone and email communications. This represents an expansion of "dataveillance" or the monitoring of "data trails" of individuals and their transactions. According to Gandy (1989, p. 62), "Modern surveillance technology is an integrated system of hardware and software including devices for sensing, measuring, storing, processing, and exchanging information and intelligence about the environment." Antiterrorism laws throughout the world have enhanced governments in their ability to use electronic surveillance for investigating terrorism and other crimes (Gellman, 2002).

According to Webster (2012) in public administration today, there has been the "normalization" of surveillance creating an x-ray vision. There are three important reasons for this. First, citizens are becoming accustomed to the fact that their personal information is not created personally by them, but by administrative agencies. Second, it has become "normal" for public agencies to create large databases of records containing personal information. Third, it has become the "normal" practice for citizens to exchange personal information in order to get access to public services. Essentially, it has almost been impossible for citizens to function without this electronic footprint.

There are several justifications for surveillance programs to fight against terrorism (Haggerty & Gazso, 2005). First, surveillance can provide information that can be used to understand the operation of terrorists. Second, surveillance can be used to deter another terrorist attack. Third, surveillance can be used to intervene in real time to prevent terrorist acts before they occur.

However, mass data surveillance has the problems of the wrong identification, unclear, inconsistent, and low quality data (Clarke, 1988). There can be the issue of spurious matches. Mass data surveillance can be an arbitrary action since authorizers have no prior suspicion, and can interfere with individual privacy (Clarke, 1988). Lyon (2003) believes that there are three issues with digital surveillance trends. First, there is a centralization of state power because of surveillance. Second, there is the capacity to discriminate between different citizens using surveillance algorithms. Third, there is a relative lack of accountability of these surveillance systems and the public generally willing to tradeoff surveillance for increased security.

In addition, one of the issues with dealing with the terrorist threat is that all levels of government and commercial entities need to share information and coordinate operations (Popp, Armour, Senator, & Numrych, 2004). There is no one organization that can have all of the information, and sharing information is critical to monitor terrorist activity and prevent future attacks. This is most notably found in the NSA with its surveillance program.

## 3. National Security Agency surveillance program

The Bush administration had authorized a large-scale electronic surveillance program after the terrorist attacks of September 11, 2001, which was called the Terrorist Surveillance Program (Bagley, 2011). The purpose of this program was to intercept and collect intelligence and evidence to prevent a future terrorist attack. The U.S. government has built a national security database from the information collected from Bellsouth, AT&T, and Verizon (Bagley, 2011).

The events of September 11 motivated the passage of legislation such as the U.S. Patriot Act of 2001 to permit greater government surveillance (Gellman, 2002; Regan, 2004). The USA Patriot Act was significant antiterrorism legislation that was adopted at the height of national emotional response to the immediate aftermath of September 11 (Haque, 2002; Strickland, 2003). The Act grants unprecedented powers to the executive to conduct surveillance through electronic means, such as gathering personal records, tracking emails, and internet usage. Critics of this law say that it enables law enforcement to invade privacy without meaningful judicial oversight (Nelson, 2002).

Jaeger (2007) argues that immediately after September 11, many federal agencies provided greater restrictions to government information through websites. This shows the extent to which there was more of a concerted effort to be more careful what information was provided online following the terrorist's attacks. Jaeger and Bertot (2010) further note that after the George W. Bush administration, Obama promised to have a greater focus on government transparency and use of new social media technologies, which means the promotion of a more citizen-centered approach for achieving better governance in public administration. One of the results of September 11 is that more mundane and everyday conversations and transactions are under increased scrutiny than ever before (Lyon, 2003).

Presently, we are in a multi-channel communication environment of increasingly complex, dynamic, mobile and big data flows around the globe Government agencies, including the National Security Agency in the U.S. (National Security Agency, 2014), are the largest collectors and generators of big data of great diversity (Janssen, 2011). Specifically, Jetzek, Avital, and Bjorn-Andersen (2013, p. 179) observe: "In the past two years alone, the data generated from internet-based transactions, surveillance cameras, and smart devices have boosted the amount of data available in the digital universe to its current rate of 2.8 ZB, a number that is expected to double every year." Here the reported rate of 2.8 ZB refers to 2.8 billion terra bytes; an incredible amount of big data.

From this new environment, for the NSA, one of the more extensive efforts to fight terrorism has been the use of data mining. Data mining, according to Gandy (2005, p. 364) "is a process that has as its goal the transformation of raw data into information that can be utilized as strategic intelligence with the context of an organization's identifiable goals." Data mining is especially important in the context of the extent that technology can be used to integrate data from previously independent data records (Gandy, 2005). Data mining can be used for the extraction of meaningful intelligence, meaning to discover what patterns emerge in a dataset (Gandy & Schiller, 2002). Data mining technology in the private sector has spread, as there has been an increased emphasis on homeland security since September 11, 2001 (Gandy & Schiller, 2002). One of the most important criticisms of the mass data surveillance is that warehousing data in a large data warehouse, and using data mining technologies, will lead to many false positives (Popp & Poindexter, 2006).