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/© 2015 Elsevier Inc. All rights reserved.

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).

This integration of data, and the greater availability of data, has provided challenges for public policy (Gandy, 2005). Some of the limitations of data mining are that it can help to determine patterns and relationships, but it does not tell us the significance of the relationship (Seifert, 2004). In addition, data mining helps to identify connections between variables, but does not determine causation. The issue of data quality is an important issue as mistaken inferences can be made with poor quality data. Finally, interoperability of data is an important issue, as data needs to be combined for further analysis.

This era of "big data" makes it a challenge to protect individual privacy and civil liberties (Mundie, 2014). Current privacy laws protect individuals and were created in a time before the internet and require valid consent for collecting data. Data collection today can use data from completely public sources that infer personal information from individuals such as age, marital status, occupation, income, and political orientation which can easily come from social networking sites (Danna & Gandy, 2002).

For example, the federal government in the U.S. has used big data that has been provided by commercial service providers, creating such databases as "no fly" lists and boarder searches (Lesk, 2013). Essentially, private data collection is subject to few constraints in the U.S. and is readily used by the federal government.

Metadata are the transaction records that are generated when you send or receive an email or text message (Sullivan, 2013). What comes from the metadata are the location of where the message was sent, when it was sent, the subject of the message, recipients of the message, and the web address of receipts. The Obama administration believes that examining metadata is within the law, since the actual content of the message is not accessed by the NSA (Tzanou, 2013). The idea is that by examining the metadata the government could identify leads of individuals or groups that might be involved in terrorism activities (Tzanou, 2013). The following section examines more closely the relationship between citizen-centric e-governance and political efficacy, the theoretical framework of this paper.

4. Citizen-centric e-governance and political efficacy

4.1. Theory of citizen-centric e-governance

In social science research, a distinction is made between theoretical and empirical concepts. The distinction and the link between theoretical propositions and theory-driven hypotheses can be shown on the theoretical and empirical levels (Bhattacherjee, 2012). Fig. 1 below shows this mapping of propositions derived from our theory of citizen-centric e-governance on the theoretical level, to our analysis of citizens' NSA issue-specific political discourses and public opinion on the empirical level. The theory suggests that citizens with greater political efficacy will have different views from those that are less involved and engaged in public affairs and policy.

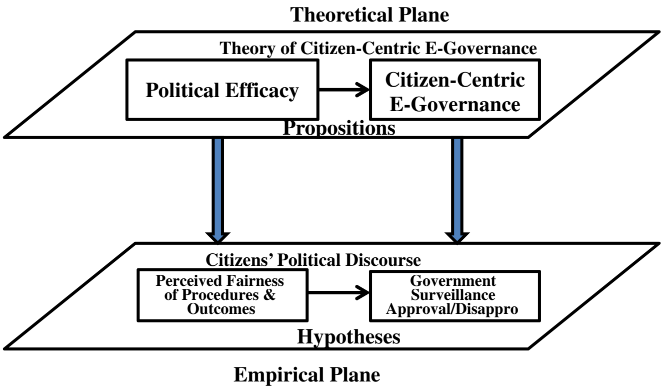
Theoretical Plane
Theory of Citizen-Centric E-Governance
Political Efficacy
Citizen-Centric E-Governance
Propositions
Citizens' Political Discourse
Perceived Fairness of Procedures & Outcomes
Government Surveillance Approval/Disappro
Hypotheses
Empirical Plane

Fig. 1. Framework of theory-driven political discourse and public opinion analysis.

Research on e-governance articulates the importance of technology to create a new relationship between citizens and their government (Reddick, 2005). With the internet, citizens can become more civically engaged and work toward the "coproduction" of government services (Linders, 2012). Traditional e-government models of technology adoption for public service delivery indicate a one-directional impact of government providing services to citizens, and citizens accepting the services they received (Reddick, 2011). Citizen centric e-governance, by contrast, argues for "we government", meaning that citizens work collaboratively with government and promote real and meaningful change together (Linders, 2012). Efforts at creating more open government and participatory government are examples of citizen-centric e-government in action (Bertot, Jaeger, & Grimes, 2010). The use of social media technologies is another example of engaging citizens in public policies.

4.2. Political efficacy, political trust, and emotion

Essential to the vibrancy of democracy and success of citizen-centric e-governance are the role played by citizen trust in government and perceptions of government responsiveness, also known as external political efficacy. The literature works to reconcile whether it is a positive trust in government or a healthy distrust in government that better engages citizen participation (see Marien & Christensen, 2013). Much of the assumption was that for democracy to be successful, citizen trust must be implicit and explicit. Citizens need to perceive fairness of political procedures and outcomes (Craig, Niemi, & Silver, 1990), along with government responsiveness (Anderson, 2010; Parent, Vandebeek, & Gemino, 2005).

A healthy skepticism, however, is found to effectively engage citizens. In their investigation of the effects of media perceptions on external political efficacy, Pinkleton, Austin, Zhou, Willoughby, and Reiser (2012, p. 32) find that rather than turning off citizens, skepticism "may lead citizens to seek additional information to find answers to their questions and confirm or disconfirm what they already have learned." For Pinkleton et al. (2012, p. 32), then, "dissatisfaction thereby leads to increased levels of efficacy, ultimately enhancing political engagement." When this healthy skepticism is combined with external political efficacy, they suggest that it produces citizens engaged in a deliberative process that more fully informs their decision-making. With NSA surveillance serving as a trigger for negative attitudes toward government, the question remains whether these negative perceptions translate into engagement and opinion formation. Given that research shows those who oppose the current administration and who perceive government monitors their internet behavior participate in politics at higher rates, we expect to find negative emotions having the effect of engaging citizens (Krueger, 2005).

Emotions play a substantial role in directing citizen expectations of government. In addition, we have seen a mix of messages citizens send government. Increased confidence in government is associated with the emotional response of individuals after September 11, 2001 (Gross, Brewer, & Aday, 2009). We also witnessed that citizens' trust in government rose to levels not seen since the mid-1960s immediately after September 11 (Chanley, 2002; Cook & Gronke, 2005). In fact, research shows that the perception of a threat significantly influences terrorism related opinions almost a decade after the September 11 attacks (Malhotra & Popp, 2012).

For e-governance, the relationship with trust and efficacy is complex, but largely associated with a positive trust (Bannister & Connolly, 2011; Tolbert & Mossberger, 2006; West, 2004). Parent et al. (2005) found internal political efficacy, more strongly than external political efficacy, determines trust levels that citizens have with their government. The findings of this research indicate that for more effective e-government policy for promoting citizens' political engagement, government needs to identify and target citizens with high prior levels of trust in government rather than allocating further resources for developing better e-government websites or portals for policy information or citizen-to-government interactions. Others argue the relationship is more complex and that citizens who are more satisfied with e-government trust the government more, while those who trust government more are also more satisfied with e-government, demonstrating an interactive effect (Welch, Hinnant, & Moon, 2005). This is consistent to the evidence by Parent et al. (2005) in which individuals with trust have this reinforced with e-government use. In contrast, the federal e-government usage did not have an impact on public trust in government in the U.S. context. While certainly gaining insight toward the complexity of the relationship, we need to consider contrary opinions to existing government policies and broadening the scope of opinions for purposes of e-governance. If those who disapprove of government and distrust government remain engaged but carry opinions different from those who trust government, they need to be enticed to participate fully in e-governance for a rounded discourse to occur.

4.2.1. Institutional and policy opinions

Nelson (2004) argues that with the increased technology in our lives there is an ongoing policy debate surrounding issues of privacy. The challenge that Nelson presents is that we must accept the presence of technology in our lives, but must continually debate what impact this has on existing democratic systems. Privacy protection is more of an issue in the digital age, because there has been a massive increase in the personal information on the web of individuals coupled with this increase in the analytical power available to commercial and governments through search engines and other means (Weitzner et al., 2008). Smith, Dinev, and Xu (2011) have labeled us in a new era of privacy development, starting in the 1990s with the rise of the internet, and Web 2.0 in the late 2000s, and the terrorist attacks of September 11, 2001 have dramatically changed the landscape of information exchanges. There has been a new level of privacy concerns expressed by the public.

Government collection of the personal data of individuals is often seen as an invasion of privacy, something that has been increasingly discussed in the e-government literature (Bannister, 2005; Belanger & Hiller, 2006). E-government applications have three types of information privacy problems, which are collection problems, use and disclosure problems, and security problems (Wu, 2014). There should be protections by government to address each of these three areas. “Information rights” are referred to in the privacy literature as the issues dealing with information activities such as the creation, management, dissemination, and use of information (Caidi & Ross, 2005).

Some have argued for information accountability, which is that information use should be transparent so individuals can determine whether a particular use is appropriate given the rules or laws set out (Weitzner et al., 2008). Individuals and institutions should be held accountable when there is misuse under information accountability. Information rights should be acknowledged as a user-centric process where citizens should be empowered to become “active citizens” (Caidi & Ross, 2005).

Gould (2002) argues that in time of national emergencies, Americans will tradeoff civil liberties for increased security. They will give the government increased latitude in surveillance. However this will change if there is mishandling by government or public administration governance failure. According to Bannister (2005) there is a tradeoff with security and privacy, which can be viewed in light of risk. The greater the level of security, the more intrusion on privacy for society. All societies must balance both security and privacy.

Research shows that while Americans support civil liberties, a majority is not convinced that a tradeoff with security is necessary (Lewis, 2005). This finding is counter to those that argue that the public is quick to provide restrictions on civil liberties; they indeed want both, especially when they fail to perceive clear and present danger. Empirical research shows that liberals are less likely to trade off civil liberties than moderates or conservatives (Davis & Silver, 2004).

Within the U.S. democratic system, then, on what institutions can citizens rely for maintaining the balance? Since the executive branch has set the policy on government surveillance, it is not surprising that those that disapprove of the president are more likely to perceive government monitoring uses as invasive techniques (Best & Krueger, 2008). However, levels of approval and disapproval have fluctuated. For example, President George W. Bush had high public approval ratings for his job performance during immediately after September 11 (Bloch-Elkon, 2007). However, presidential approval decreased by 20 points from 2004 to 2005. From the days of the attack to two months after there was two thirds of Americans that had a “great deal” or “a good amount” of confidence in their government to prevent similar attacks on American soil. Americans became gradually less confident in government to prevent a terrorist strike four years after September 11.

In the case of NSA surveillance, we have the added effect of the media acting as a source of control over the abuse of government and information rights (Caidi & Ross, 2005). The media, then, adds an additional check, although not formal, to the U.S. democratic system. The following section presents the findings of our multi-method research approach.

5. Multi-method research findings

In this section, we describe two research methods used for our analysis of the NSA surveillance program and their key findings. The first method is the political discourse analysis of #nsa tweets. Here we examine tweets on the NSA surveillance program after the Edward Snowden revealed the metadata collection program of the NSA. This section research method examines Twitter data and shows the major influencers in this blogosphere. For the second research method, examine data from a Pew survey asking Americans what their approval/disapproval of the NSA surveillance program. We use the information to derive a model of approval/disapproval of the NSA surveillance program in which we test a statistical model. The purpose of using these two research methods is to be able to explore the issue more comprehensively rather than relying on just one method.

5.1. Political discourse analysis using online social networks

Online social networks are computer-mediated virtual communities whose members share common interests, needs, or purposes. On the voluntary basis, members produce user-generated information content, including text and images, for the consumption and the re-use by other network members. Social network analysis (SNA) has been used in biomedical (Bales, Johnson, & Weng, 2008; Jonnalagadda, Peeler, & Topham, 2012), tourism (Baggio, 2008; Ying, 2010), e-government (Chung & Chatfield, 2011), and disaster management (Cheong & Cheong, 2011).

Twitter, a type of microblogging and social media platform, now has more than half a billion active account holders worldwide, with more than 140 million users in the U.S. alone. Twitter adopts a strategy to offset the 140-character limit of tweets by introducing the hashtag symbol (#) to direct the focus of tweets and enable Twitter users to categorize their tweets by #keyword. This strategy reduces transaction costs by facilitating greater efficiency, for example, in searching specific political information or specific-issue political discourses to participate via Twitter sphere. While a tweet can contain several hashtags to show that it has many foci to highlight, Twitter suggests a tweet to have no more than 2 hashtags. Hashtags then have a link to a search result with the hashtag as the keyword (Chatfield & Brajawidagda, 2012).

While it is unclear when #nsa was first created within Twitter sphere, its use among Twitter users became markedly noticeable on June 5 2013, when The Guardian revealed the unauthorized leak of classified NSA documents by the former NSA contractor, Edward Snowden. The Guardian published its first Snowden's leak, revealing a secret court order showing that the U.S. government had forced Verizon to hand over the phone records of millions of Americans. Essentially, the NSA's mass surveillance programs became public knowledge on June 5, for the first time, revealing an order from the Foreign Intelligence Surveillance Court (FISC) on April 25, 2013 requiring Verizon Business Network Services to provide NSA to hand over metadata from millions of Americans' phone calls, to the Federal Bureau of Investigation (FBI) and the NSA (The Guardian, 2013a). On June 6 a second Guardian story reveals the existence of the previously undisclosed program Prism, which internal NSA documents claim gives the agency "direct access" to data held by Google, Facebook, Apple and other U.S. internet giants.

5.1.1. Twitter data collection

As discussed, a rapid increase in the use of #nsa was very unmistakably noticeable on June 5, 2013 among Twitter users, in the immediate aftermath of the reported unauthorized leak of national security documents by the former NSA contractor. While political discourses still continue on a slower pace into 2014, we have limited our data collection, through Topsy.com, to the month of June 2013 due to the large volume of tweets with #nsa being exchanged in Twitter sphere.

Topsy.com, a real-time search engine, indexes billions of tweets for social web analytics. Its website, however, seems to limit the download capacity to 10,000 tweets per time interval which a person or a computer program selects. Therefore, we have selected time interval of 30 min to maximize the number of tweets downloaded from topsy.com, while minimizing the total download time. In order to optimize the random sampling strategy of #nsa tweets, a computer program has requested a download of #nsa tweets every 30 min in interval. For our critical discourse analysis, we downloaded 226,884 tweets, which were issued by 83,253 unique Twitter users who engaged in specific-issue political discourses using #nsa during the month of June 2013.

5.1.2. Political discourse analysis of #nsa tweets

By embedding #nsa in their tweets, the 83,253 unique Twitter users, during the month of June 2013, signaled their political interest in issues related to NSA surveillance programs – more openly and more transparently – than other Twitter users who have not been aware of or have decided not to use #nsa. Therefore, it is relevant and value-adding for us to study the dynamic virtual community formed by the emerging ad hoc social networks of #nsa users for NSA related political discourses.

Fig. 2 shows a time series graph of #nsa trending for the month of June 2013 using Twitter's streaming API for all the 226,830 tweets with #nsa. In applying critical discourse analysis to ad hoc social networks, where nodes and links dynamically change over time, it is helpful for us to visualize overall patterns of #nsa discourses along two dimensions: (1) time and (2) political interest and engagement in specific issues related to NSA surveillance programs among the #nsa users. In Fig. 2, the x-axis shows time (day as a unit of measurement) as a reference line for the y-axis. The y-axis shows the number of tweets with #nsa per day (the sum of all #nsa tweets issued during 24 h). In our study, we use this y-axis value as a proxy for estimating the level of political interest and engagement in issues related to NSA surveillance programs among the #nsa users.

Our analysis of #nsa trending indicates that the level of the online citizens' political interest in NSA surveillance programs and their Twittersphere political discourses has not been static or constant over time. Fig. 2 seems to indicate three waves. In the first wave, the level of political interest and engagement suddenly and explosively increased from 287 #nsa tweets on June 5 2013 to the first peak of 13,113 #nsa tweets on June 8. This heightened-level was sustained for 10 days till June 14. In the second wave, the level of the online citizens' political interest in NSA surveillance programs and their Twittersphere political discourses seem to be on the decline until June 17 and the level increased on June 19. Finally, the third wave shows further decline but it has not dropped to the pre-June 5 baseline (the average of 120 #nsa tweets) toward the end of our data collection period. With 6791 #nsa tweets on June 29 and 1866 on June 30, our analysis indicates that a lower-level but sustained political interest and engagement in #nsa discourses has been displayed by the online citizens.

Table 1 shows the observed peaks in Fig. 2 which seem to correlate with the most plausible critical events reported by major newspapers in the context of NSA surveillance programs. The critical events were identified through keyword search (National Security Agency OR NSA), with our search period limited to the month of June 2013, using FACTIVA academic database which contains major newspaper articles worldwide.

5.1.3. Citizens' political discourses: key findings

Table 2 below reports the descriptive statistics which indicate that of 83,253 unique users of #nsa, a fairly large percentage of users (69.3%) engaged in this specific-issue political discourses inactively by contributing only one tweet during the month of June. This indicates, with Twitter, similarly to traditional media, that there are dominant groups of individuals that contribute most of the tweets and perhaps direct the conversation limiting widespread political discourse and citizen engagement. They also indicate that the top 10 most active users, as the collective, contributed a total of 5809 tweets (2.6% of the total 226,830 we downloaded). Given the large dataset file (28 MB) and the practical

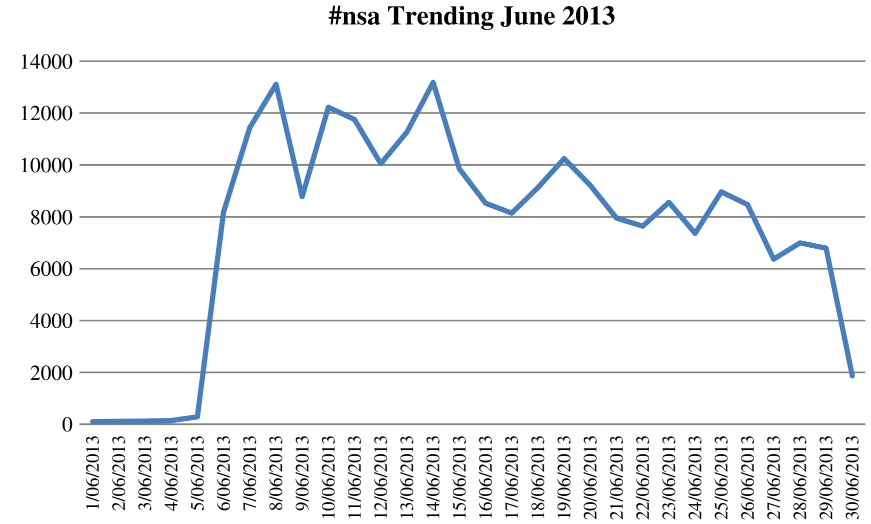

Fig. 2. #nsa trending during the month of June 2013.

Table 1
Critical events for Twitter discourse analysis.

Wave	Peak	Critical event reported/date	Reference
1	June 5	"Leak of classified NSA documents"/June 5	The Guardian (2013a)
	June 8	"NSA is collecting phone records of Verizon customers", resulting in the U.S. Foreign Intelligence Surveillance Court order/June 6 "Reports on U.S. surveillance of Americans fuel debate over privacy, security", further fueling for critics of NSA surveillance programs/June 7 "U.S. agents tapping servers of leading internet companies"/June 7 Note: Section 215 provision of the 2001 USA Patriot Act requires companies to turn over business records.	Reuters News (2013a) Reuters News (2013b) Reuters News (2013c)
1	June 10	"Rand Paul and the rise of the libertarian Republican"/June 10 Note: Edward Snowden: He did it because "it's important to send a message to government that people will not be intimidated." Note: National Intelligence Director James Clapper: the leaks were ""literally gut-wrenching" and cost the intelligence community dearly".	The Washington Post (2013)
1	June 14	"N.S.A. leaker says he will fight extradition in Hong Kong", revealing NSA hacking globally/June 12 Note: Edward Snowden: "We hack network backbones – like huge internet routers, basically – that give us access to the communications of hundreds of thousands of computers without having to hack every single one." "POLL-Across U.S., nearly half say government spying OK within limits", Reuter opinion survey findings/June 13	The New York Times (2013) Reuters News (2013d)
2	June 19	"Obama does not feel Americans' privacy violated — chief of staff"/June 17 Note: President Obama's chief of staff on CBS's "Face the Nation" program said: "President Barack Obama does not believe the recently disclosed top-secret National Security Agency surveillance of phone records and internet data has violated Americans' privacy rights." "Obama says will meet oversight board about NSA surveillance"/June 18 Note: In his PBS interview, President Obama stated he would meet: "a privacy and civil liberties oversight board to discuss ways to balance the need for U.S. surveillance while respecting people's right to privacy". "NSA chief: U.S. spy program disclosure caused 'irreversible' damage"/June 19	Reuters News (2013e) Reuters News (2013f) Reuters News (2013g)
3	June 25	"GCHQ taps fibre-optic cables for secret access to world's communications"/June 22	The Guardian (2013b)

page limitation of this paper, in the next section, we discuss our findings of political discourse analysis on the top 10 most active #nsa users, as well as some notable politicians and mass media reporters who engaged in #nsa discourses.

5.1.4. Political efficacy

We used two operational definitions of political efficacy in performing critical discourse analysis of the 5809 #nsa tweets issued by the ten most active #nsa users during the month of June 2013. Table 3 below shows some examples of their #nsa tweets and our classification of these tweets into either one of the two operational definitions of political efficacy: FP and GR. Here FP refers to perceived fairness of government procedures and outcomes (or the lack thereof), whereas GR refers to perceived government responsiveness to citizens' concerns and demands (or the lack thereof).

As Table 3 indicates, the eight out of the ten most active #nsa users in this Twitter sphere, which has its central focus on NSA surveillance related political discourses, have identified either the absolute or the relative lack of perceived fairness of government (or NSA) procedures. Two out of the eight have astutely observed the perceived political and institutional risk of government (or NSA) outsourcing highly sensitive technological programs to private-sector third-party contractors. The IT outsourcing practice has been widely diffused among governments not only in the U.S. but also worldwide. This practice has given rise to the unauthorized release of top-secret government documents by Edward Snowden, a former employee of the third-party contractor to NSA. Moreover, they have also voiced their concerns about the lack of the transparent and tangible benefits (or delivered positive outcomes) of the NSA surveillance programs in terms of the fight against global terrorism.

Table 2
Descriptive statistics of #nsa tweets and #nsa users.

Descriptive statistics	Dataset analyzed
Minimum number of #nsa tweet per user	1
Maximum number of #nsa tweets per user	1058
Average number of #nsa tweets per user	2.7
Top 10 users contributed to	5809 #nsa tweets (2.6%)
Top 100 users contributed to	20,372 #nsa tweets (9.0%)
Top 1000 users contributed to	60,853 #nsa tweets (26.8%)
Top 2000 users contributed to	79,631 #nsa tweets (35.1%)
Number of #nsa users who issued only one tweet during the month of June 2013	57,679 (69.3%)
3366 out of the total 83,253 users contribute 10 or more #nsa tweets, totaling	95,649 out of the total 226,830 #nsa tweets (42.2%)
Language in use	Largely in English (Twitter users whose citizenship clearly discernible from U.S., UK, Canada, and Australia) but also in German, French, Spanish, Japanese, and Korean

In contrast, the eight most active #nsa users have been rather silent about perceived government responsiveness to citizens' concerns and demands or the lack thereof, except one #nsa user who is critical of President Obama's (lukewarm) responsiveness to the scale and scope of the NSA surveillance programs revealed by Snowden and sensationally reported by mass media worldwide.

5.1.5. Citizen-centric e-governance

As discussed earlier in this paper, the construct of citizen-centric e-governance has been operationally defined for the online survey analysis to include citizens' approval or disapproval of government surveillance or more specifically NSA surveillance programs. We have used this operational definition in our critical discourse analysis of the #nsa tweets issued by the ten most active #nsa users. Table 4 below shows our findings of #nsa tweets on #nsa users' approval or disapproval of the NSA surveillance programs.

Our analysis of a sample of the #nsa tweet data indicates that all of the top ten active #nsa users have shown their propensity to distrust government and disapprove NSA surveillance programs and their intelligence collection as the act of "evil" and "lying" government targeted specifically against citizens.

On the one hand, they all seem to have emotionally responded to the mass media's sensational reports, starting on June 5, on NSA spying on all American citizens and/or their technological and institutional capabilities to even escalate the scope and scale of intelligence collection operations, without scrutinizing these reported "facts". This is evidenced by the level of time and emotional intensity they have

Table 3
#nsa tweets on political efficacy.

#nsa users (total of #nsa tweets issued during the month of June 2013)	#nsa tweets (time, wave & user-generated content)	FP	GR
FBF (1058)	Note: This Twitter account name and its 1058 #nsa tweets throughout the three waves indicate that this account holder (or Twitter bot — a computer program) has demonstrated no political knowledge or serious interest in this NSA specific issue discourse.		
KRFront (823)	14/06/2013 4:48 (W1):http://t.co/W7W4PmrnfR — giving rogue low level government "intelligence" agencies something to read. #irs #prism #patriot #nsa 19/06/2013 6:51 (W2): Give the #NSA something to read @KRFront #nsa #irs #patriot #krf 25/06/2013 0:01 (W3): Give the #NSA something to read @KRFront #nsa #irs #patriot #krf 5 Note: Despite the high-level volume (823) #nsa tweets issued by KRFront, none of the tweets contain either of perceived fairness of government procedures and outcomes or perceived government responsiveness.		
GD (818)	20/06/2013 6:59 (W2): Greenwald: #NSA Director is 'Misleading' the public http://t.co/m7QRJkPkDv #fisa #prism #privacy #rights #snowden #surveillance #tcot #tgdn 19/06/2013 7:24 (W2): #Fisa court oversight: a look inside a secret and empty process http://t.co/KQ98Gmghce #nsa #prism #privacy #rights #snowden #surveillance 25/06/2013 0:16 (W3): They charge #Snowden with #espionage, and cooperate with foreign powers to spy on their own people. #nsa #gchq #prism #snowden #tempora	☑ ☑ ☑	
DP (561)	7/06/2013 14:55 (W1): #NSA can acquire the content of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. 7/06/2013 21:35 (W1): RT @FearDept: Suppose someone asserted their rights. The more data we have on them, the easier to find a crime that fits their profile.#NS… McGill_83CANADA, 20/06/2013 7:05 (W2): RT @deanprocter: #NSA Memo: Remind the public how #NSA surveillance helped capture Osama Bin Laden so quickly.	☑ ☑ ☑	
M97 (474)	19/06/2013 3:51 (W2): One of the biggest concerns everyone should have is the majority of work for #NSA is done by corporations whose bottom line is PROFIT Note: She astutely identifies perceived political, institutional and societal risks associated with government outsourcing of top security technical projects to private-sector contractors, including Booz Allen, Edward Snowden's employer. 19/06/2013 4:40 (W2): RT @_cypherpunks_: #NSA releases new explainers on 215 and 702 and their oversight. 215: http://t.co/gTv5cLGUIj 702: http://t.co/Dj3XpEM4Ll… 19/06/2013 5:38 (W2): RT @democracynow: .@ggreenwald tells us "the most vehement and vicious attacks" on his reporting "come from Democratic partisans." http://t… 19/06/2013 5:59 (W2): Now @CNN is stating that NSA thwarted 50 terrorist attacks. That is not what #NSA said &amp; I do not believe what NSA really said. 19/06/2013 20:52 (W2): RT @JameelJaffer: Must-read by @ggreenwald about the 2008 FISA Amendments Act and the #NSA's monitoring of Americans' phone calls. http://t…	☑ ☑ ☑ ☑	☑
TT (469)	12/06/2013 14:17 (W1): PLEASE: See short 8/2012 vid "The Program" on #NSA's HUGE DOMESTIC spying. William Binney is apologetic. http://t.co/eeM0ZyWmiP @csmagor TPO_Hisself, 12/06/2013 21:19 (W1): RT @velvethammer: Joe Biden 2006: Bush #NSA Collecting Phone Records "Very, Very Intrusive" [Video] http://t.co/9yfJ7S1Dku #PRISM #FISA #tc… 13/06/2013 14:58 (W1): Digital Blackwater: How #NSA Gives Private Contractors Control of Surveillance State| 70% of spending to #MIC http://t.co/R2mMs4Dqe6 #tcot #p2 19/06/2013 7:24 (W2): #NSA MT @drichi2009 The Sickening Snowden Backlash: http://t.co/8KWPBahlxI 19/06/2013 9:15 (W2): #NSA stories forcing way more transparency than we've ever had;https://t.co/E2qzU5KZuC …@NomDePlume9 @ggreenwald @suigenerisjen @trevortimm	☑ ☑ ☑ ☑ ☑	
VF (434)	7/06/2013 23:55 (W1): U voted for him, not I: @cenkuygur: Obama has done untold damage by institutionalizing programs that were considered radical under Bush #NSA 10/06/2013 0:07 (W1): RT @SenRandPaul: Is 1984 Now? Big Brother is watching http://t.co/lmCCS80wZA #LostTrust #IRS #PRISM #NSA #coleg #bospoli #masen 20/06/2013 0:37 (W2): President's #FBI Director Admits He Uses Spy Drones On Americans In America http://t.co/DfiSmUZ7Wq #NRA #IRS #NSA #tcot #bospoli #coleg	☑ ☑ ☑	

FD (410)	13/06/2013 18:30 (W1):
	RT @AJEnglish: Opinion: The recent #NSA leak reveals the extent to which the U.S.' government and corporate sectors have merged | http://t.co…
	14/06/2013 9:23 (W1):
	RT @sdmattpotter: #NSA case provokes new criticism of huge role played by #intelligence contractors http://t.co/3V4QRqsZZH via @publici
		☑
		☑	

EW (394)	14/06/2013 21:41 (W1):
	Senators challenge NSA's claim to have foiled 'dozens' of terror attacks What about #Boston? http://t.co/fbX6jzNbyR #NSA #tcot #ccot #ctot
	14/06/2013 21:55 (W1):
	RT @WashTimes: Germany decries NSA surveillance as 'Stasi methods' — Washington Times http://t.co/SZHtceb7rs #NSA
		☑	

I59 (368)	8/06/2013 13:44 (W1): Obama Dismisses Concerns Over #NSA Mass Surveillance Programs, SEN. JEFF MERKLEY STRONGLY REBUTS — Dem Underground http://t.co/KUwTppDkYf 8/06/2013 13:41 (W1): USA Today 5/11/2006 — '#NSA has massive database of Americans' phone calls — "Democratic Underground http://t.co/0zrnPgjZkm #PoliceState" 8/06/2013 17:22 (W1): Exclusive: Top whistleblower spills the beans on the real extent of the #NSA spying http://t.co/g7KF8IRydX Using Israeli cos to do it	☑ ☑	☑

FP: perceived fairness of government procedures and outcomes (or the lack thereof).
GR: perceived government responsiveness (or the lack thereof).
RT: re-tweet other's tweet.

engaged in the #nsa Twittersphere from June 6 to June 30 2013. On the average, they issued 23 tweets daily, ranging from 42 (FBF) to 15 (I59) per day.

On the other hand, they all seem to have elevated Edward Snowden as "the hero" who has fought against the "evil" and "lying" government. They all discounted or ignored the fact that he had been legally charged

Table 4
#nsa tweets on approval/disapproval of NSA surveillance programs.

#nsa users (total of #nsa tweets issued during the month of June 2013)	#nsa tweets (time, wave & user-generated content)	A	D
FBF (1058)	Note: No single relevant #nsa tweet has been found to indicate either approval or disapproval of the NSA surveillance programs, despite the highest volume of #nsa tweets issued by FBF.		
KRFront (823)	Note: KRFront largely refers others to read its publication against government surveillance.		☑
GD (818)	26/06/2013 20:27 (W3): @Duchwela You should be more circumspectful about the normalization of evil. #Privacy violation is not acceptable. @Aine #nsa #snowden		☑
DP (561)	9/06/2013 3:58 (W1): James Clapper would have us think #NSA surveillance is legal, just like the way they treated #Manning is 'legal', like torture is 'legal'. 20/06/2013 17:45 (W2): RT @Europarl_EN: "We cannot allow Americans to spy on EU citizens" — @EP_Justice discusses #Prism project by U.S. secret service #NSA http://…		☑ ☑
M97 (474)	19/06/2013 5:59 (W2): Now @CNN is stating that NSA thwarted 50 terrorist attacks. That is not what #NSA said &amp; I do not believe what NSA really said. 19/06/2013 11:42 (W2): #NSA Scandal: How Leaks Advance Liberty and Resist Tyranny — http://t.co/5Gtmqgjug6http://t.co/VF3xVnjUpi 19/06/2013 20:40 (W2): RT @guardian: #NSA surveillance is an attack on American citizens, says Noam Chomsky http://t.co/pMt1bgcyT6 #NSAfiles		☑ ☑ ☑
TT (469)	19/06/2013 7:29 (W2): Those who tell us loudly to 'trust Govt!' are a part of the now fairly-transparent con that is itself destroying our trust in Govt. #NSA 19/06/2013 9:42 (W2): At least I take it you are for MORE transparency abt #NSA @NomDePlume9 @ggreenwald @trevortimm @ suigenerisjen 19/06/2013 11:30 (W2): RT @RepThomasMassie: We must never accept the premise that government can lie to us for our own good. It's time for Clapper to resign.#NSA …		☑ ☑ ☑
VF (434)	10/06/2013 6:42 (W1): #NSA Whistle Blower: A Disillusioned Obama Voter Who Said: "I Believed His Promises." #PRISM #IRS #p2 #p2b #topprog #CTL #LDS #tcot #Bain 19/06/2013 22:49 (W2): This President Earned America's Distrust. Truth Leaked Out In Spite Of State-Controlled Media. #NRA #IRS #NSA #p2 #bospoli #coleg #masen		☑ ☑

FD (410)	13/06/2013 18:51 (W1):
	RT @MaribelLafuente: Stand with Edward #Snowden! @BarackObama — stop #NSA spying and get out of our email. Sign the petition and RT https:…
	TuxcedoCat, 19/06/2013 3:21 (W2):
	Me, too. RT @BashirLive 'I'm uncomfortable with how much credence we've given to one 29-year-old man.' @finneyk #Snowden #NSA
		☑	☑

EW (394)	10/06/2013 6:38 (W1):
	RT @FoxieNews: Edward Snowden is being Charged with Espionage! Wait, they're going after the wrong guy! OBAMA should be in cuffs! #NSA #PRI…
	10/06/2013 6:55 (W1):
	RT @Surabees: #EdwardSnowden is an inspiration for those who want to hold the Government accountable to the people http://t.co/4KZsl9T7TB #…
	19/06/2013 0:02 (W2):
	RT @sirtatters: #BENGHAZI IS BEING STALLED BY #IRS #NSA ASK WHY #NSA DIDNT RESPOND DURING #BENGHAZI OR #BOSTON TERROR @RepMikeRogers @Darr…
	25/06/2013 0:37 (W3):
	Stand with Edward #Snowden! @BarackObama — stop #NSA spying and get out of our email. Sign the petition and RT https://t.co/nuFudOdsrk
			☑
			☑
			☑
			☑

I59 (368)	8/06/2013 11:13 (W1): This is our biggest chance in a year. Stoke the fires, spread the word. #NSA Mass Surveillance. http://t.co/EYdIysnurD #tlot dwill6413, 8/06/2013 13:31 (W1): RT @Ian56789: If you're OK with revelations of #NSA snooping, you're part of the problem — Democratic Underground http://t.co/LfjuODtQRu #P… 8/06/2013 17:57 (W1): #NSA Mass Surveillance This is NOT a partisan issue This is a right from wrong issue And it's plain WRONGhttp://t.co/EYdIysnurD #p2 #tcot 9/06/2013 8:30 (W1): The #NSA Mass Surveillance programs are an impeachable offense for @BarackObama for abuse of power #p2 #tcot http://t.co/hwXk6X9fpl		☑ ☑ ☑ ☑

A: approval of NSA surveillance programs.
D: disapproval of NSA surveillance programs.
RT: re-tweet other's tweet.

for the theft of the top secret U.S. government documents and he had to seek for overseas governments' protection where their own citizens do not have the same level of the liberty and privacy as the U.S. citizens do. Interestingly, in the #nsa Twittersphere, the top ten most active #nsa users have discussed neither the inherent tradeoffs between national security and citizens' liberty and privacy nor how best government might use the collected intelligence and big data (e.g., metadata on mobile and internet communications) for enhanced national security.

5.2. Public opinion poll findings

The discourse analysis, our first research method provides the above insight on the dialogue occurring in one type of social media. We now investigate through our second research method, public opinion data. We investigate these insights further within the greater U.S. adult public (18 years and older). For our statistical analysis, we utilize the Pew Research Center for the People & the Press survey conducted July 17–21, 2013 to examine the effects of trust and efficacy on opinions of NSA surveillance. The telephone interviews were administered via landline and cellphone to a nationally representative sample of 1480 United States adults. We weigh the data to correct for the demographic discrepancies identified.

Importantly, the Pew survey operationalizes key variables of interest. These include citizen approval or disapproval of government metadata collection, levels of citizen trust in government institutions, perceptions of government transparency and the role of the media, assessments of the progress the U.S. government has made in fighting terrorism along with perceptions citizens have about whether government has encroached on individual liberties. Finally, the survey captures political elements, such as a measure of presidential approval and partisanship. Appendix A provides the operationalization of each of our variables of interest.

5.2.1. Dependent variable

Our primary dependent variable measures overall approval or disapproval of the government's data collection policy. Responses were coded 0 if respondents approved and 1 if respondents disapproved. Importantly, 52.7% of respondents approved of the government's data collection policy while 47.3% disapproved. This is a contrast to the findings from the discourse analysis. Overwhelmingly, the discourse analysis revealed a disapproval of the policy while the broader public appears more split. However, what informs these policy opinions?

5.2.2. Independent variables

Our selection of independent variables is guided by the literature as well as the insight provided in the Twitter discourse analysis. As discussed below, we organize our 11 independent variables into four broad concepts: institutional checks, terrorism policy, role of the media, and political affiliation.

5.2.2.1. Institutional checks. Given the U.S. government structure of separated branches of government, we were concerned with U.S. citizen perceptions of the checks in place and presidential power. One idea being that presidents may exert more or less influence on the other institutions of government and directions of public policy, depending on their standing with the public (Edwards, 1997). Another idea being that the public is capable of holding the president accountable for policy decisions and outcomes (Ostrom & Simon, 1985). Given that the surveillance policy was a manifest of the executive branch, we utilize a measure of presidential approval. We believe that greater presidential disapproval would lead to greater disapproval of the NSA surveillance program. When presidential approval is high, presidents have more latitude in policies that they can implement, and this was witnessed with the high approval rating of George W. Bush after September 11, 2001. Importantly, 50% of respondents approved of the way Barack Obama was handling his job as President while an even 50% disapproved.

However, could other branches keep the overextension of that policy in check? The Pew survey asks respondents to consider whether the federal courts provide adequate limits on what telephone and internet data the government can collect? With 65.3% of respondents answering that the courts do not provide an adequate limit on what government can collect, U.S. public opinion indicated a lack of faith in the courts as a viable check. However, assessment of the courts was mostly favorable. Respondents were asked of their overall opinion of the federal courts with 55.8% answering very favorable or mostly favorable.

5.2.2.2. Terrorism policy. We make use of four different aspects of the public's views toward the U.S. government's terrorism policy, as captured by Pew. For one measure, respondents were asked about their views on the U.S. government's terrorism policy. Respondents were generally favorable in their assessment of the U.S. government's success, with 69.3% of respondents saying that the U.S. government is doing very well or fairly well.

A second question probes respondents to consider the U.S. government's terrorism policy as it pertains to civil liberties. Several concerns about the infringement by the U.S. government on U.S. civil liberties emerged in the discourse analysis. Importantly, a majority, 57.2%, believed government had gone too far in restricting the average person's civil liberties, while 42.8% believed the government had not gone far enough to protect the country.

An additional key insight that emerged from the discourse analysis is the question of the purpose for which government has engaged in the data collection. To understand this concept within the greater U.S. public, we include a measure that captures U.S. public opinion associated with the purpose the government data collection method serves and whether the intent of the policy is solely directed at fighting terrorism. Public skepticism was glaring, with only 24.1% of respondents indicating that the data collection was only being used to fight terrorism and 76% indicating that the government uses this data for purposes other than fighting terrorism.

To measure U.S. citizen opinions of government transparency, respondents were asked if “government keeps too much information about its anti-terrorism programs secret from the public.” Given that the transparency question is directed toward the government's terrorism policy, we have included it in the terrorism block of variables. Approximately 59% agreed with the statement and believe that government keeps too much information secret, lacking transparency while approximately 41% disagreed.

5.2.2.3. Role of the media. Media has long been considered a check on the institutions of the U.S. government and it was a leak by a media source that generated broader concerns about the U.S. government's metadata collection policies. In fact, some of the tweets from the discourse analysis above reference media sources. Therefore, we utilize two questions to capture perceptions of the role of the media. One question asks if “the news media reports too much information that can harm the effectiveness of the government's anti-terrorism programs” which is coded 0 if respondents agreed and 1 if respondents disagreed. Approximately 56% responded that they agreed with the statement, while approximately 44% responded they disagreed.

A second question asks if respondents “think the news media should – or should not – report information it obtains about the secret methods the government is using to fight terrorism.” Responses are coded 0 if respondent answers “Yes, should” and 1 if respondent answers “No, should not.” Given the media's role in revealing the level of government surveillance, it is interesting to note that respondents are fairly evenly split with almost 50% responding that the news media should report the lack of transparency by government when it comes to fighting terrorism, while approximately 50% respond they should not report this information.

5.2.2.4. Political affiliation. Given that partisan preferences could skew the perceptions of the government's metadata policy, we control for partisan influences using a measure of party identification. Approximately 20% of respondents self-identified as Republican, with almost 31% self-identifying as Democrat, while the greatest proportion, 49%, self-identified as Independent.

5.2.3. Multivariate analysis

Based on the dichotomous coding for our dependent variable, we use binary logistic regression (logit) to estimate the independent effects on the probability of U.S. citizen disapproval of government data collection (Table 5). The model correct case classification rate is 74.4%. This indicates that our independent variables included in this logit model can classify the public's approval/disapproval views rather effectively. All variables are statistically significant and in the expected direction, except for the assessment of government transparency and the emergence of the distinction between Republicans and Independents. Republicans are more likely than Independents to disapprove the U.S. government's data collection program. When accounting for the combined effects in the model, some notable odds ratios emerge.

With regard to trust in the institutions of government, respondents who do not believe the courts provide adequate limits on the data the U.S. government can collect are six times more likely than those who have trust in the courts to limit the government's policy to disapprove of the data collection. Also, for those citizens who are distrusting of the U.S. government's intent, those who believe the data collection serves a purpose beyond fighting terrorism are almost twice as likely as those who believe the U.S. government is using the data collection solely for the stated purpose of fighting terrorism to disapprove

Table 5
Logit analysis of the U.S. public's disapproval of government metadata collection.

	B (se)	Exp(B)
Institutional checks		
Courts provide limits	1.55*** (.10)	4.71
Federal courts' approval	.23*** (.05)	1.26
Presidential approval	.56*** (.10)	1.75
Terrorism policy		
Inadequate response to terrorism	.15** (.05)	1.16
Violate civil liberties or not far enough	−.97*** (.09)	.38
Data use (terrorism or other)	.65*** (.12)	1.92
Government transparency	−.17	.85
Role of the media		
Media reporting doesn't harm	.56*** (.09)	1.73
Media should not report secrets	−.48*** (.10)	.62
Political affiliation		
Republic	.27* (.12)	1.31
Democrat	.23* (.11)	1.26
Constant	.03***	
−2Log likelihood	3134	
LR Chi^2	957***	
Nagelkerke pseudo-R-square	.37	
N	757	

Logistic regression coefficients are reported along with standard errors in parentheses.
p < .10.
* p < .05.
** p < .01.
*** p < .001.

the government's data collection. Finally, those who believe that the news media's reporting did not threaten the U.S. government's anti-terrorism programs were also almost twice as likely to disapprove the government's data collection program.

Overall, the statistical analysis reveals that a similar pattern emerges, supportive of the discourse analysis above. The consequences that emerge are a general distrust in institutions of government to keep each other in check along with a continued role for the media in keeping the U.S. accountable. In addition, threats to civil liberties and distrust in the U.S. government's motives continue to have far reaching implications.

6. Discussion and conclusion

The findings of our Twitter discourse analysis and logistic regression of a public opinion survey revealed consistent and generally negative sentiments toward the NSA surveillance programs. This was especially evident in the very high level of #nsa tweets during the month of June, when Edward Snowden, the former NSA contractor, first leaked the government metadata collection program to the media. From our political discourse analysis, this showed three distinct waves representing releases to the media and the response of the Obama administration. Our results indicated that eight out of the ten most active #nsa users on Twitter have identified either the absolute or the relative lack of perceived fairness of NSA procedures. Our analysis #nsa tweet data further indicated that all of the top ten active #nsa users have shown their propensity to distrust government and disapprove NSA surveillance programs as going against the rights of citizens. Interestingly, while the literature on government surveillance mentioned in our literature review section has indicated issues of citizens trading off national security and civil liberty as important, they were not evident in our Twitter discourse analysis. This demonstrates the differences in gathering public opinion through surveys compared to social media. With public opinion surveys there are efforts to create a random sample to provide broad representation of the population. While Twitter's specific hashtag has been designed to attract those who are interested in the specific topic the hashtag indicates, with a tendency toward a self-selection bias. Within the hashtag users, those with the greatest number of followers can exert influence in directing the conversation, and hence making the tradeoff difficult to detect.

Our statistical analysis of the public opinion poll of Americans revealed that actually there were more people who approved (52.7% of respondents) than disapproved of the surveillance programs. However, when examining the Twitter blogosphere, we did not witness much approval at all. This most likely is the result of the differences in those on the Twitter blogosphere who are more likely to be opinion makers, while the Pew survey is more representative of the larger population in the U.S. Another plausible reason may be the disparity in political affiliation represented by the survey. While prior research shows that Republicans tend to disapprove the Administration's surveillance program, only 20% of the survey respondents self-declared as Republican in comparison to much higher percentages of Democrats (31%) and Independents (49%), respectively. The logistic regression models did show that many of the most important political efficacy variables such as institutional checks, views and reaction to government policy, the media, and political party affiliation impacted the disapproval of the surveillance program. From our statistical analysis, institutional checks and terrorism policy had the greatest impact on disapproval levels. In general, those who are skeptical of government institutions, and the goals of the terrorism policy, more highly disapprove of the NSA metadata surveillance program.

Overall, citizens who are more engaged, and exhibit politically efficacious behavior, are more likely to disapprove the surveillance policy, with a facilitating role for the media. Importantly and consistent with what others have found, the negative perceptions did not disengage citizens. Rather, an outcry is apparent in the discourse analysis. 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. For e-governance, our findings suggest that those with distrust in government, not only remain engaged, but hold different policy perspectives. For e-governance to truly be citizen-centric, competing views need to be incorporated into the process. However, there are other channels where citizens can be engaged such as email, calls to elected officials, public forums, among others. The difficulty is in identifying the most productive method for incorporating these opinions. Drawing out contrary opinions requires advocates of e-governance to use creative methods for soliciting and incorporating a balance of perspectives.

This study shows the importance of using multiple methods to answer important but previously insufficiently examined research questions. We witnessed this with the tweets we analyzed, having a much more one-sided view of the NSA surveillance program. However, the statistical analysis of the Pew public opinion data revealed the importance of politics and policy on the disapproval of the program. The Twitter analysis was used as an important tool to inform a better-specified model in our statistical analysis. Both research methods showed the importance of political efficacy on creating a more engaged public, thus creating more citizen-centric e-governance. While we have long known that citizen feedback in the form of negative assessments of government programs and actions is not always what those governing wish to hear, it is exceedingly important for government to cultivate citizen-centric e-governance through which a productive feedback-loop can help government better balance national security and citizens' privacy and civil liberties. Such a citizen-centric e-governance mechanism seems to be vital to further developing more open and more transparent government. Toward this goal, we have shown preliminary evidence of the utility of our proposed theory of citizen-centric e-governance in addressing the contentious issues of public importance; namely citizens' views on government surveillance programs.

There are some limitations of this research that should be mentioned. First, since we used a preexisting survey instrument, we are limited in the questions that we can ask. Second, we had a limited sample of tweets analyzed; as a result some important information may have been left out of our Twitter discourse analysis. Third, when comparing responses from a survey sample with comments from Twitter this represents different opinions. Twitter contains more what we have seen with opinion makers, while our survey sample is more representative of the general population of the U.S.

Despite these limitations this was an exploratory study showing that Twitter data has difficulty using this medium to make significant statement, but offers a different range of opinions, which you may not get through an examination of the traditional media outlets. In addition, comparing Twitter data with public opinion survey data shows that with a public opinion survey, this is broadly representative of the population and more varied, but Twitter data is more influenced by the major opinion makers. We believe that with our use of multi-method approach, we can more effectively understand the complexity in diverse public opinion on the NSA surveillance programs, which would be rather difficult through the use of a single research method for our analysis.

Appendix A. Operationalization of variables

	Coding	Pew survey question
Variables		
Approval/disapproval of government's data collection method	0 = approve 1 = disapprove	Overall, do you approve or disapprove of the government's collection of telephone and internet data as part of anti-terrorism efforts?
Institutional checks		
Courts provide limits	0 = do provide adequate limits on what government can collect 1 = do not provide adequate limits on what government can collect.	Do you think federal courts do or do not provide adequate limits on what telephone and internet data the government can collect?
Federal courts' approval	1 = very favorable 2 = mostly favorable 3 = mostly unfavorable 4 = very unfavorable.	Would you say your overall opinion of The Supreme Court is very favorable, mostly favorable, mostly unfavorable or very unfavorable?
Presidential approval	0 = approve 1 = disapprove	Do you approve or disapprove of the way Barack Obama is handling his job as President?
Terrorism policy		
Inadequate response to terrorism	1 = very well 2 = fairly well 3 = not too well 4 = not at all well	In general, how well do you think the U.S. government is doing in reducing the threat of terrorism?
Violate civil liberties or not far enough	0 = that they have gone too far in restricting the average person's civil liberties 1 = that they have not gone far enough to adequately protect the country.	What concerns you more about the government's anti-terrorism policies?
Data use (terrorism or other)	0 = only being used to investigate terrorism 1 = the government uses this data for purposes other than terrorism investigations.	Do you think this government data collection effort is only being used to investigate terrorism, or do you think the government uses this data for purposes other than terrorism investigations?
Government transparency	0 = agreed 1 = disagreed	Government keeps too much information about its anti-terrorism programs secret from the public.
Media		
Media reporting doesn't harm	0 = agreed 1 = disagreed	The news media reports too much information that can harm the effectiveness of the government's anti-terrorism programs
Media should not report secrets	0 = yes, should 1 = no, should not	Do you think the news media should – or should not – report information it obtains about the secret methods the government is using to fight terrorism?
Political		
Republic	0 = Independent 1 = Republican	In politics today, do you consider yourself a Republican, Democrat, or Independent?
Democrat	0 = Independent 1 = Democrat	

References

Anderson, M. R. (2010). Community psychology, political efficacy, and trust. *Political Psychology*, *31*(1), 59–84.

Baggio, R. (2008). *Network analysis of a tourism destination*. University of Queensland Australia.

Bagley, A. W. (2011). Don't be evil: The fourth amendment in the age of Google, national security, and digital papers and effects. *Albany Law Journal of Science and Technology*, *21*(1), 153–191.

Bales, M. E., Johnson, S. B., & Weng, C. (2008). Social network analysis of interdisciplinarity in obesity research. *AMIA Annual Symposium*, *870*.

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity*, *10*(1,2), 65–78.

Bannister, F., & Connolly, R. (2011). Trust and transformational government: A proposed framework for research. *Government Information Quarterly*, *28*(2), 137–147.

Belanger, F., & Hiller, J. S. (2006). A framework for e-government: Privacy implications. *Business Process Management Journal*, *12*(1), 48–60.

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, *27*, 264–271.

Best, S. J., & Krueger, B. S. (2008). Political conflict and public perceptions. *Journal of Information Technology and Politics*, *5*(2), 191–212.

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices.* USF Tampa Bay Open Access Textbooks Collection. Book 3 (http://scholarcommons.usf.edu/oa_textbooks/3).

Bloch-Elkon, Y. (2007). Trends: Preventing terrorism after the 9/11 attacks. *The Public Opinion Quarterly*, *71*(1), 142–163.

Brown, I., & Korff, D. (2009). Terrorism and the proportionality of internet surveillance. *European Journal of Criminology*, *6*(2), 119–134.

Caidi, N., & Ross, A. (2005). Information rights and national security. *Government Information Quarterly*, *22*(4), 663–684.

Chanley, V. A. (2002). Trust in government in the aftermath of 9/11: Determinants and consequences. *Political Psychology*, *23*(3), 469–483.

Chatfield, A. T., & Brajawidagda, U. (2012). Twitter tsunami early warning network: A social network analysis of Twitter information flows. *23rd Australasian Conference on Information Systems, 3–5 Dec 2012, Geelong, Victoria, Australia*.

Cheong, F., & Cheong, C. (2011). Social media data mining: A social network analysis of tweets during the Australian 2010–2011 floods. In P.B.S., & S. Gregor (Eds.), *15th Pacific Asia Conference on Information Systems (PACIS)* (pp. 1–16). Brisbane, Australia: Queensland University of Technology.

Chung, K. S. K., & Chatfield, A. T. (2011). An empirical analysis of online social network structure to understand citizen engagement in public policy and community building. *International Journal of Electronic Governance*, *4*(1), 85–103.

Clarke, R. A. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512.

Cook, T. E., & Gronke, P. (2005). The skeptical American: Revisiting the meanings of trust in government and confidence in institutions. *The Journal of Politics*, *6*(3), 784–803.

Craig, S. C., Niemi, R. G., & Silver, G. E. (1990). Political efficacy and trust: A report on the NES pilot study items. *Political Behavior*, *12*(3), 289–314.

Danna, A., & Gandy, O. H., Jr. (2002). All that glitters is not gold: Digging beneath the surface of data mining. *Journal of Business Ethics*, *40*(4), 373–386.

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science*, *48*(1), 28–46.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance— An empirical investigation. *Journal of Strategic Information Systems*, *17*(3), 214–233.

Edwards, G. C., III (1997). Aligning tests with theory: Presidential approval as a source of influence in Congress. *Congress and the Presidency*, *24*(2), 113–130.

Gandy, O., Jr. (1989). The surveillance society: Information technology and bureaucratic social control. *Journal of Communication*, *39*(3), 61–76.

Gandy, O. (2005). *Data mining, surveillance, and discrimination in the post-9/11 environment, in the New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press 363–384.

Gandy, O., & Schiller, H. (2002). Data mining and surveillance in the post-9.11 environment. *Political Economy Section, IAMCR, Barcelona, July*.

Gellman, R. (2002). Perspectives on privacy and terrorism: All is not lost—Yet. *Government Information Quarterly*, *19*(3), 255–264.

Gould, J. B. (2002). Playing with fire: The civil liberties implications of September 11th. *Public Administration Review*, *62*(SI), 74–79.

Gross, K., Brewer, P. R., & Aday, S. (2009). Confidence in government and emotional responses to terrorism after September 11, 2001. *American Politics Research*, *37*(1), 107–128.

Haggerty, K. D., & Gazso, A. (2005). Seeing beyond the ruins: Surveillance as a response to terrorist threats. *The Canadian Journal of Sociology*, *30*(2), 169–187.

Haque, M. S. (2002). Government responses to terrorism: Critical views of their impacts on people and public administration. *Public Administration Review*, *62*(SI), 170–180.

Jaeger, P. T. (2007). Information policy, information access, and democratic participation: The national and international implications of the Bush administration's information politics. *Government Information Quarterly*, *24*(4), 840–859.

Jaeger, P. T., & Bertot, J. C. (2010). Transparency and technological change: Ensuring equal and sustained public access to government information. *Government Information Quarterly*, *27*(4), 371–376.

Janssen, K. (2011). The influence of the PSI directive on open government data: An overview of recent developments. *Government Information Quarterly*, *28*(4), 446–456.

Jetzek, T., Avital, M., & Bjorn-Andersen, N. (2013). Generating value from open government data. *Proceedings of the Thirty Fourth International Conference on Information Systems (ICIS), Milan, Italy*.

Jonnalagadda, S., Peeler, R., & Topham, P. (2012). Discovering opinion leaders for medical topics using news articles. *Journal of biomedical semantics*, *3*(1), 2.

Krueger, B. S. (2005). Government surveillance and political participation on the internet. *Social Science Computer Review*, *23*(4), 439–452.

Lesk, M. (2013). Big data, big brother, big money. *IEEE*, *11*(4), 85–89.

Lewis, C. W. (2005). The clash between security and liberty in the U.S. response to terror. *Public Administration Review*, *65*(1), 18–30.

Linders, D. (2012). From e-government to we-government: Defining a typology for citizen coproduction in the age of social media. *Government Information Quarterly*, *29*(4), 446–454.

Lyon, D. (2003). Technology vs 'terrorism': Circuits of city surveillance since September 11th. *International Journal of Urban and Regional Research*, *27*(3), 666–678.

Malhotra, N., & Popp, E. (2012). Bridging partisan divisions over antiterrorism policies: The role of threat perceptions. *Political Research Quarterly*, *65*(1), 34–47.

Marien, S., & Christensen, H. S. (2013). Trust and openness: Prerequisites for democratic engagement? *Democracy in transition: Political participation in the European Union* (pp. 109–134). New York: Springer.

Mundie, C. (2014). Privacy pragmatism: Focus on data use, not data collection. *Foreign Affairs*, *28–38*(1).

National Security Agency (2014). National Security Agency. Retrieved from http://www.nsa.gov/public_info/_files/speeches_testimonies/GC_Georgetown.pdf

Nelson, L. (2002). Protecting the common good: Technology, objectivity, and privacy. *Public Administration Review*, *62*(SI), 69–73.

Nelson, L. (2004). Privacy and technology: Reconsidering a crucial public policy debate in the post-September 11 era. *Public Administration Review*, *64*(3), 259–269.

Ostrom, C. W., Jr., & Simon, D. M. (1985). Promise and performance: A dynamic model of presidential popularity. *The American Political Science Review*, *79*(2), 334–358.

Parent, M., Vandebeek, C. A., & Gemino, A. C. (2005). Building citizen trust through e-government. *Government Information Quarterly*, *22*(4), 720–736.

Pinkleton, B. E., Austin, E., Zhou, Y., Willoughby, J. F., & Reiser, M. (2012). Perceptions of news media, external efficacy, and public affairs apathy in political decision making and disaffection. *Journalism & Mass Communication Quarterly*, *89*(1), 23–39.

Popp, R., Armour, T., Senator, T., & Numrych, K. (2004). Countering terrorism through information technology. *Communications of the ACM*, *47*(3), 36–43.

Popp, R., & Poindexter, J. (2006). Countering terrorism through information and privacy protection technologies. *IEEE*, *4*(6), 24–33.

Reddick, C. G. (2005). Citizen interaction with e-government: From the streets to servers? *Government Information Quarterly*, *22*(1), 38–57.

Reddick, C. G. (2011). Citizen interaction and e-government Evidence for the managerial, consultative, and participatory models. *Transforming government: People, process, and policy*, *5*(2), 167–184.

Regan, P. M. (2004). Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly*, *21*(4), 481–497.

Reuters News (2013 June 6a). *NSA is collecting phone records of Verizon customers —Report*. FACTIVA.

Reuters News (2013 June 7b). *Reports on U.S. surveillance of Americans fuel debate over privacy, security*. FACTIVA.

Reuters News (2013 June 7c). *U.S. agents tapping servers of leading Internet companies*. FACTIVA.

Reuters News (2013 June 13d). *POLL-Across U.S., nearly half say government spying OK within limits*. FACTIVA.

Reuters News (2013 June 17e). *Obama does not feel Americans' privacy violated —Chief of staff*. FACTIVA.

Reuters News (2013 June 18f). *Obama says will meet oversight board about NSA surveillance*. FACTIVA.

Reuters News (2013 June 19g). *NSA chief: U.S. spy program disclosure caused 'irreversible' damage*. FACTIVA.

Seifert, J. W. (2004). Data mining and the search for security: Challenges for connecting the dots and databases. *Government Information Quarterly*, *21*(4).

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1016.

Strickland, L. S. (2003). Civil liberties vs. intelligence collection: The secret Foreign Intelligence Surveillance Act court speaks in public. *Government Information Quarterly*, *20*(1), 1–12.

Sullivan, J. L. (2013). Uncovering the data panopticon: The urgent need for critical scholarship in an era of corporate and government surveillance. *The Political Economy of Communication*, *1*(2).

The Guardian (2013a). Guardian announces leak of classified NSA documents, June 5, 2013. Retrieved from http://www.theguardian.com/world/2013/jun/05 (accessed on June 5 2013)

The Guardian (2013b). GCHQ taps fibre-optic cables for secret access to world's communications. June 22 2013. Retrieved from http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

The New York Times (2013). N.S.A. leaker says he will fight extradition in Hong Kong. Retrieved from http://www.nytimes.com/2013/06/13/world/asia/nsa-leaker-says-he-will-stay-in-hong-kong-and-fight-extradition.html?_r=0

The Washington Post (2013 June 10). Rand Paul and the rise of the libertarian Republican. Accessed from http://www.washingtonpost.com/blogs/the-fix/wp/2013/06/10/rand-paul-and-the-rise-of-the-libertarian-republican/

Tolbert, C. J., & Mossberger, K. (2006). The effects of e-government on trust and confidence in government. *Public Administration Review*, *66*(3), 354–369.

Tzanou, M. (2013). Is data protection the same as privacy? An analysis of telecommunications metadata retention measures. *Journal of Internet Law*, *17*(3), 21–34.

Webster, C. W. R. (2012). Surveillance as X-ray. *Information Polity*, *17*(3–4), 251–265.

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). Information accountability. *Communications of the ACM*, *51*(6), 82–87.

Welch, E. W., Hinnant, C. C., & Moon, M. J. (2005). Linking citizen satisfaction with e-government and trust in government. *Journal of Public Administration Research and Theory*, *15*(3), 371–391.

West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public Administration Review*, *64*(1), 15–27.

Wu, Y. (2014). Protecting personal data in E-government: A cross-country study. *Government Information Quarterly*, *31*(1), 150–159.

Ying, T. (2010). *Social networks in the tourism industry, an investigation of Charleston, South Carolina, Clemson University*. South Carolina, USA: Clemson University.

Dr. Christopher G. Reddick is a Professor and Chair of the Department of Public Administration at the University of Texas at San Antonio, USA. His research and teaching interests are in information technology and public sector organizations. He serves as an editor-in-chief of the International Journal of Public Administration in the Digital Age. He has widely published his research work in *Public Administration Review*, *Government Information Quarterly*, *Public Organization Review*, *International Journal of Civic Engagement and Social Change*, *Public Performance and Management Review*, *International Journal of Public Administration*, *International Journal of E-Politics*, *Information Polity*, *Transforming Government: People, Process and Policy*, *International Journal of Services Technology and Management*, *Information Technology for Development* and others. He currently serves as a guest co-editor for the *Journal of Homeland Security and Emergency Management* Special Issue on ICT and Crisis, Disaster and Catastrophe Management with Dr. Akemi T. Chatfield.

Dr. Akemi Takeoka Chatfield has earned her M.B.A. and Ph.D. in Business Administration (MIS & Management Sciences *summa cum laude*) from Texas Tech University in the U.S. She is currently the Director of E-Government & E-Governance Research at the University of Wollongong in Australia. She was a visiting Professor at Kyoto University Disaster Prevention Research Institute under the 2010 Extreme Weather Conditions Research Program funding. She was invited as a keynote speaker for the *2010 E-Governance World Summit* in Taipei, Taiwan. Her research interests include crisis response and management, networked organizations, network technology benefits realization, social media in government, social network analysis, big data and social media analytics, open government policy, government transparency and collaborative forms of governance. She published in *Journal of Management Information Systems*, *European Journal of Information Systems*, *Journal of Information Systems Frontier*, *Communications of the ACM*, *Data Base*, *Information Technology for Development Journal*, *International Journal of Electronic Governance*, *Electronic Journal of E-Government*, *Government Information Quarterly* and *International Journal of Public Administration in the Digital Age*. She currently serves as a guest co-editor for the *Journal of Homeland Security and Emergency Management* Special Issue on ICT and Crisis, Disaster and Catastrophe Management with Professor Christopher G. Reddick.

Dr. Patricia A. Jaramillo is presently a lecturer in the Department of Public Administration at The University of Texas at San Antonio, located in San Antonio, Texas. She holds a PhD in Political Science from the University of Colorado at Boulder. Her research interests include civic engagement, political participation and Latina/o politics and participation and she has publications around these interests.