GUEST EDITORIAL PREFACE

Special Issue on Information Technology and Homeland Security

Christopher G. Reddick, Department of Public Administration, The University of Texas at San Antonio, San Antonio, TX, USA

This special issue for the *International Journal of E-Politics* examines the important issue of information technology (IT) and its impact on homeland security. We focus specially on the politics and policy of IT on homeland security, examining cases in the United States, Europe, and in several developing countries. The five papers in this special issue provide the reader with some of the most important concerns in IT and Homeland security, such as the need for democratic governments to accountable to their citizens, at the same time as creating surveillance societies because of potential terrorist threats.

The term homeland security has become commonplace after the terrorist attacks on the World Trade Center and Pentagon on September 11, 2011. The U.S. government, in fact, created the largest single department since World War II entitled the Department of Homeland Security, recognizing the importance of preventing a future terrorist attack on U.S. soil. When we discuss homeland security, we take a view that terrorism of course is an important element here. However, history shows that securing the homeland is also related to responding to natural disaster, such as Hurricane Katrina and Sandy, since these events have great spillover effects across the a country and world. The collection of papers in this special issue addresses both the terrorism aspects of IT and homeland security and the importance of emergency management.

Although there have been numerous studies that examine homeland security and its impact on government preparedness and response, there is much less research that examines the impact of IT on homeland security. In this digital age, we increasingly need to secure vulnerable infrastructure and protect citizens from a terrorist attack. IT becomes a means to secure infrastructure, and enables governments to more effectively help citizens in the event of a terrorist attack or natural disaster.

There are five papers in this special issue which discuss various aspects of IT and homeland security. The first paper by Regan and Monahan examine the U.S. Department of Homeland Security fusion centers, which share data across government agencies as well

as across the public and private sectors. This paper examines, through interviews of key officials, what organizational-legal factors shape the data-sharing practices of fusion centers. The creation of fusion centers, have precipitated an environment in which information is not just used for counterterrorism but also to solve all crimes. These fusion centers are essentially able to "connect the dots" in that collaboration and the use of data is a critical function for the prevention of a terrorist attack or other crimes. This paper shows that many public programs, such as fusion centers, start out with a specific mission, in this case to share data to prevent a terrorist attack, and evolve to a much broader mission of helping in all crimes. These authors note, one of the challenges moving forward with fusion centers, is that they tend to facilitate data-collection, data mining, and pattern-searching activities that are in conflict with existing privacy laws.

The second paper in this special issue by Kitsos and Yannoukakou examines whether privacy and openness can coexist and the conditions necessary for its coexistence. There has been a movement especially Europe and North American for open data practices and cloud computing which promise a more efficient, transparent, accountable, accessible, and democratic governance. However, open government raises many concerns in regards to privacy. The difficulty with open government are that the years followed the September 11, 2011 terrorist attacks, we have seen an erosion of privacy and data protection. Their paper discussed the inherent tension between preventing a future terrorist attack and providing more open and accessible government. According to these authors, the adopted laws and policies only marginally safeguard the right to privacy and enable governments to collect immense amount of personal data through the telephone (mobile or fixed), Internet, airline passenger information, and banking information, all in the name of terrorism. These authors note that privacy and personal data protection are major issues that must be safeguarded without sacrificing national security and public interest on one hand, but without crossing the thin line between protection and infringement on the other.

The third paper by Rahm and Reddick examines, through a survey, factors identified in the literature that are said to impact IT and emergency management. These factors are political and organizational, IT used for emergency management, social media and emergency management, and knowledge and data management. This study found that these four factors were an issue for the delivery of emergency services in the Texas emergency management. Politics, resource constraints, and traditional organizational forms each played a role in the adoption and use of IT. IT seemed to be most useful during the response stage of emergency management as is evidenced by the heavy reliance on Geographic Information Systems (GIS) and mapping. Social media was not shown to be very influential and when used and was not used to its full potential to enable larger participation from public bystanders. Knowledge and data management were important to the Texas emergency service districts, especially in terms of data security and protection of privacy. This paper shows the important of using IT in communicating with citizens especially in times of crisis.

In the paper by Dahah, this author explores panopticon and panspectron using the case study of the Israeli controlled Palestinian territory, the Gaza Strip. While the panopticon is concerned primarily with individual surveillance and control, the panspectron is about mass surveillance and control of society. The conclusion of this author is that the Gaza case study may indicate what is to come with the use of IT to create "authoritarian democracies," where the state reorganizes itself around an increasingly authoritarian surveillance society. As a result, civil liberties are eroded and reduced democratic oversight are exchanged for the promise of greater security. Dahah, similar to Regan and Monahan's paper shows the inherent tension in civil society with surveillance and democratic accountability in the fight against terrorism.

The final paper is this special issue is by Saeed, Malik, and Wahab. These authors exam-

ine Pakistan, which is on the front line with the U.S. in the war against terror. In the post 9/11 World, homeland security has become focal issue for every country and governments are constantly improving security mechanisms to protect their citizens. Pakistan is heavily affected country by terrorism within the country and in surrounding countries. This paper specifically examines Pakistani security agency websites to evaluate usability aspects. Survey results highlighted that these websites have several usability problems, which need to be rectified before they could effectively be used. The main contribution of the paper is usability analysis of security agencies websites in Pakistan is very problematic, generally being uninformative for citizens.

Christopher G. Reddick
Guest Editor
IJEP

Christopher G. Reddick is Professor and Chair of the Department of Public Administration at the University of Texas at San Antonio. His research and teaching interests are in information technology and public sector organizations. He is also author of Homeland Security Preparedness and Information Systems, which deals with the impact of information technology on homeland security preparedness.