Editorial Preface

Vishanth Weerakkody, Brunel Business School, Brunel University, Middlesex, UK

It is my pleasure to introduce Volume 12, Issue 3 of the International Journal of Electronic Government Research. This issue of IJEGR presents five papers focusing on established and emerging themes within the context of e-government. The research covered in this issue include information security in e-government, open data and its influence on e-government, e-government training programs, the role of trust in the context of e-government and Online Voting Systems in government. While issue such as trust, security and voting have been widely debated in e-government studies, the influence of open data in the context of e-government and research into e-government training programs are areas that are emerging and need further study. In particular, several emerging studies have questioned the public value and usefulness of open data to citizens as well as the usability of data offered on open data portals. Similarly, the area of e-government training programs, whether reflecting on experiences of delivery or developing frameworks for such programs, is an area that has been neglected in the e-government literature. Conversely, the areas of trust and security have been widely explored, yet new findings and propositions continue to emerge both from contextual and conceptual perspectives. In this context, it is hoped that the research reported in this issue of IJEGR will contribute to strengthening established areas of exiting research into e-government and help further develop emerging areas within the field.

The first paper introduced in the issue is by Eunjung Shin and Eric Welch and is entitled 'Socio-technical Determinants of Information Security Perceptions in US Local Governments.' This paper examines the social mechanisms influencing electronic information security and applies a socio-technical framework to model how technical, organizational and environmental complexities limit electronic information security. The paper also examines to what extent organizational design buffers security risks. The study empirically validates the proposed framework in the context of U.S. local government's online media use using data collected from local government managers. The study concludes that technical complexity, and organizational and environmental complexities are negatively associated with local managers' awareness of electronic information security.

The second paper is authored by Rui Pedro Lourenço and is entitled 'Evidence of an open government data portal impact on the public sphere.' This paper aims to find evidence of the impact of open government portals and discover whether citizens and other stakeholders actually use the information offered in these portals. The paper adopts a qualitative content analysis approach and finds that data disclosed through a portal is used for a wide range of purposes: including monitoring resource misuse and public spending overview analysis, to discuss specific contracts and spending options, to hold public agents accountable in what concerns the tendering process, the outputs and the outcomes of governmental actions, to prevent and denounce possible cases of corruption or nepotism, and to support arguments within broader policy discussions occurring in the public sphere.

The third paper is entitled 'Developing E-Government Training Program.' In the paper authors Annie DA Abdullah, Calvin ML Chan and Syamimi Ariff Lim investigate the development of an e-government training program using stakeholder theory. A two-stage process model is proposed and is analyzed using case study data to provide a theoretical explanatory basis for the process of developing e-government training programs and practical guide for practitioners. The authors claim that the propositions put forward in the paper offers a foundation and reference for future research to develop theoretically-based approaches to advance the state of e-government education research.

The fourth paper is by Mahmood Khosrowjerdi and is entitled ‘Trust in People, Organizations, and Government.’ This paper explores different types and aspects of trust in previous studies to shape a more generic model for trust. The Trust model presented by the authors consists of three-tiers. The first tier designates three major levels of trust: Individual (micro), Institutional (meso), and Governmental (macro). The second tier differentiates seven kinds of trust relationships in society: Person-to-Person(s), Person-to-Organization(s), Person-to-System(s), Person-to-Government, Organization-to-Organization(s), Organization(s)-to-Government, and Government-to-Government(s). The third tier describes the related concepts and aspects of trust at each level of society.

The final paper in this issues of IJEGR is by Lauretha Rura, Biju Issac and Manas Kumar Haldar and is entitled ‘Implementation and Evaluation of Steganography based Online Voting System.’ The authors introduce a novel approach to enhance E2E (end-to-end) voting system security by combining visual cryptography with image steganography. The study collected surveys from 30 random participants to measure the user acceptance of a newly developed software, which was developed using a high level of usability testing and user acceptance testing. The paper concludes that new e-government systems, when developed with user involvement and feedback at both design and testing phases, are likely to be favoured and accepted by citizens when introduced to replace an existing government process.

I hope that the papers offered in this issue of IJEGR have answered or attempted to answer important research questions and/or address practical problems and challenges in the field of e-government that the readers find useful.

Vishanth Weerakkody
Editor-in-Chief
IJEGR