Challenged Democracies: The Impact of Digital Government on Democracy and Democratic Institutions

John Carlo Bertot
University of Maryland
jbertot@umd.edu

Karine Nahon
IDC Herzliya
knahon@idc.ac.il

Paul Jaeger
University of Maryland
pjaeger@umd.edu

1. Introduction

Through the years, Digital Government research has focused on a range of topics, including government practice, policy implications and frameworks, technologies, governance, engagement, and other matters related to technology-enabled government. Within and among those topics, Digital Government research has focused on such areas as inter-operationalization, administrative modernization, citizen engagement, transparency and openness, participation in democratic processes, and more [1, 2, 3, 4].

Overall, the published research identifies the challenges and opportunities that digitally-enhanced government brings with it in general, and on modern platforms such as social media in particular. Little, if any, attention has been given to the dangers that Digital Government brings to democracy and democratic societies. In recent years, democratic societies have witnessed the [5, 6, 7, 8, 9, 10, 11]:

- "Closing" of government through selective and/or altered release of government data.
- Attacks on government institutions and credibility by the governing via digital platforms such as social media.
- Rise of anti-democratic uses of social media by governments and political figures.
- Attack on democratic elections and leaders though falsified content on social media platforms.
- Falsification of government reports and information and/or the attack on the credibility of government data by those within government power.

2. Goals of the Minitrack

This minitrack explores concerns with digital government applications, implementations, and practice. More specifically, the minitrack moves away from an often optimistic perspective of open, transparent, and engaged digital government to address questions such as:

- In what context and circumstances do applications and uses of digital government may threat or harm institutions of government, citizens, and others in the public sphere?
- What is the impact of social media platforms in democracies in general and on participation and representation in liberal democracies in particular?
- In what ways algorithms or artificial intelligence biases extend vulnerabilities of democracies? What are the available solutions to such implications?
- What strategies, policies, and other efforts can, do, or should governments, citizens, civic groups, and others engage in to ensure democratic principles in the face of potential threats from technology-enabled government?
- What is the impact of big-data analysis and surveillance by public sector or intermediaries on privacy principles?
- What are the implications for adopting innovative uses of social media from non-government contexts to the government context?
- Are social media platforms increasingly another branch of government that require 'checks and balances'?
- In what ways do online power dynamics impact the electoral systems in democracies?
- What are the implications for government use of digital technologies that provide inaccurate information to the public and/or sound false alarms in emergency or security-related matters?

HŤCSS

- What are the considerations and implications for open, but potentially biased, data?
- How do governments engender trust in the institutions of governments in an era of "fake news" and "alternate facts" increasingly promoted and enabled via digital sources?

3. Papers

In the paper "Does Online Political Participation Reinforce Offline Political Participation?: Using Instrumental Variation" Sung and Jang explore whether online political participation can predict the strengthening of offline political participation by using privacy concerns as an instrumental variable. Their study found that age and ideological inclination were more important factors in offline political participation than socioeconomic status. Further, their study suggests that online political participation reinforces offline political participation. Perhaps significantly, their findings suggest that online participation activities can reinforce offline political participation and that it is possible to mobilize groups that were alienated from offline political participation. The findings have implications for engaging marginalized groups in the democratic process.

Gu, Harrison, and Zhu investigate the use of information dissemination and public communication by Chinese municipal governments. Their study analyzed the social media use of three large Chinese cities with relatively mature social media development in order to ascertain the effect of social media use in citizen engagement. The findings of their study suggest that there is not necessarily a relationship between the number of government social media postings, citizen responses, and engagement. Indeed, the results of the study show that there is a limited relationship between posts and responses, suggesting that governments there is a need for governments to look beyond simply using and posting on social media in order to attract citizens feedback, achieve two-way communication goals, and foster robust democratic participation.

citizens.the lack of knowledge and trust in official authorities and privacy concerns in relation to public participation in public discourse in their paper entitled "The Role of Pseudonymity in Mobile e-Participation." Their paper uses a long-term field study with a mobile participation prototype, to

The paper "Vice or Virtue? Exploring the Dichotomy of an Offensive Security Engineer and Government 'Hack Back' Policies" by Withers, Parrish, Smith, & Ellis explores the use of "red hat" hackers to proactively seek security weaknesses in systems as a means to strengthen cybersecurity measures and methods. "Red hat" hackers differ from the better-known "white -hat" hackers in applying the methods of cybercriminals against cybercriminals and counter or preemptively attacking, rather than focusing on defending against attacks. The paper uses the virtue (ethics) theory and cyber attribution to argue that there exists a dichotomy among offensive security engineers, one that appreciates organizational security practices, but at the same time violates ethics in how to retaliate against a malicious attacker.

4. References

[1] Criado, I., Sandoval-Almazan, R., & Gil-Garcia, J.R. (2013). Government innovation through social media. *Government Information Quarterly*, 30(4): 319-326.

[2] Ambrose-Oji, B., van der Jagt, A. P., & O'Neil, S. *Citizen Science: Social Media as a supporting tool*. Available at: https://www.forestry.gov.uk/pdf/Social_Media_Support_Citizen_Science_April_2014.pdf/$FILE/Social_Media_Support_Citizen_Science_April_2014.pdf.

[3] Panagiotopoulos, P., Bowen, F., & Brooker, P. (2017). The value of social media data: Integrating crowd capabilities in evidence-based policy. *Government Information Quarterly*, 34(4): 601-612.

[4] Brabham, D. C. (2008). Crowdsourcing as a model for problem solving: An introduction and cases. *Convergence*, *14*(1), 75-90.

[5] Bekkers, V., Edwards, A., & de Kool, D. (2013). Social media monitoring: Responsive governance in the shadow of surveillance? *Government Information Quarterly*, 30(4): 335-342.

[6] Mauriello, T. (2017, February 22). Government watchdogs criticize Trump's removal of open data sets. Pittsburgh Post-Gazette. Available at: http://www.govtech.com/data/Government-Watchdogs-Criticize-Trumps-Removal-of-Open-Data-Sets.html.

[7] Union of Concerned Scientists. (2017). Sidelining Science Since Day One. Washington, DC: Center for Science and Democracy, Union of Concerned Scientists. Available at: https://www.ucsusa.org/sites/default/files/attach/2017/07/sidelining-science-report-ucs-7-20-2017.pdf.

[8] Madrigal, A.C. (2018, June 4). What We Know About Facebook's Latest Scandal. *The Atlantic*. Available at: https://www.theatlantic.com/technology/archive/2018/06/what-we-know-about-facebooks-latest-data-scandal/561992/.

[9] Sanders, J., & Patterson, D. (2018, May 31). Facebook Data Privacy Scandal: A Cheat Sheet. TechRepublic.

Available at:
https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.

[10] Intelligence Community Assessment. (2017, January 6). Assessing Russian Activities and Intentions in Recent US Elections [ICA 2017-01D]. Washington, DC. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf

[11] Howard, P.N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2018). The IRA, Social Media and Political Polarization in the United States, 2012-2018. Working Paper 2018.2. Oxford, UK: Project on Computational Propaganda. Available at: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report-2018.pdf.