

Chapter 36

Ethical and Privacy Implications of the Use of Social Media During the Eyjafjallajökull Eruption Crisis

Hayley Watson

Trilateral Research and Consulting, UK

Rachel L. Finn

Trilateral Research and Consulting, UK

ABSTRACT

In a relatively new area of research for crisis management, this article presents a discussion of some of the privacy and ethical implications surrounding the use of social media in the event of a crisis. The article uses the travel chaos caused by the eruptions of the Eyjafjallajökull volcano in 2010 to contextualise the analysis. It begins by providing an overview of the use of social media in crisis management, before continuing to present two case studies of the use of social media by members of the public and the aviation industry during the crisis caused by the ash plume. The article then proceeds to examine some select ethical and privacy implications stemming from the use of social media such as privacy infringements and inequality. The article concludes by briefly summarising the findings and considering next steps for future research in this area.

INTRODUCTION

The use of social media during a crisis to assist one another has been seen in countless emergency situations across the globe. This article utilises two case studies surrounding the use of social media during the eruption of the Eyjafjallajökull volcano in March and April 2010 to highlight preliminary findings and future research efforts that are necessary to begin to construct an understanding of the ethical, privacy and data protection impacts of the use of social media in an emergency situation.

DOI: 10.4018/978-1-5225-8897-9.ch036

The findings of this paper stem from work conducted for the European Commission funded project, COSMIC – “The contribution of social media in crisis management”. The project kicked-off in April 2013, and aims to assist first responders, including emergency services, humanitarian organisations and members of the public in using new ICT applications. It will do so by providing a set of instructions and recommendations to European stakeholders based on best practices in the use of new media in emergency situations.

During the present research, authors collected literature including news articles (including blog posts), industry reports and peer-reviewed journal articles to examine how social media was used throughout the period of time when chaos hit travelers as a result of the eruption of the Eyjafjallajökull volcano. Because the consideration of the ethical, privacy and data protection impacts of the use of these ICTs for crisis situations is a relatively unexplored area, the authors relied on the identification of ethical and privacy issues associated with similar ICT tools and applications used in different contexts (e.g., social media applications for crowdsourcing, location based technologies for advertising, etc.). This enabled a consideration of whether, and how, similar ethical issues were applicable to the use of these tools for crisis response.

This article will proceed by first providing further contextual information relating to the known uses of social media in crisis management, it will then identify how, specifically, social media was used (and by whom) during the eruption of the Eyjafjallajökull volcano. The authors then go on to identify some of the associated privacy and ethical implications of the use of social media in this case study. The article concludes by briefly summarising the findings of the paper and considering next steps for future research in this area. We argue that whilst the use of social media and other technologies provide some individuals with important information and assistance in a crisis, the potential ethical and privacy issues associated with these tools require further examination before they are unquestioningly deployed in crisis communication and crisis management contexts.

SOCIAL MEDIA AND CRISIS RESPONSE

As the use of social media in crisis management has escalated, a number of studies have demonstrated the various uses, benefits and challenges associated with this. Examples include (but are not limited to): the 2007 Virginia tech shootings (Vieweg et al., 2008), the 2007 California Wildfires (Novak & Vidoloff, 2011), the 2009 H1N1 pandemic (Nakki et al., 2011), Cyclone Yasi in Australia and New Zealand in 2011 (Taylor et al., 2012) and more recently during hurricane Sandy in 2012 (Yeomans, 2012) and the Boston Marathon bombing in 2013 (Watson & Wadhwa, forthcoming).

To illustrate, in a study that assessed the use of social media following the Virginia Tech shootings in 2007, Vieweg et al. (2008) focused on the use of the social network site Facebook for informal information gathering and problem solving activities of the public. Elsewhere, a study by Taylor et al. (2013) of social media usage following Cyclone Yasi in Australia and New Zealand in 2011 provided evidence to show how members of the public were increasingly turning to social media for updated information regarding unfolding events, demonstrating that in some cases individuals do not solely look to traditional sources of information (e.g., from news broadcasters) for information, but rather are actively seeking information from the web. Similarly, a study by the American Red Cross (2010) revealed that social media sites were the fourth most popular source that citizens accessed for emergency information.

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/ethical-and-privacy-implications-of-the-use-of-social-media-during-the-eyjafjallajokull-eruption-crisis/228754

Related Content

Early Detection of Security Holes in the Network

N. Ambika (2023). *Perspectives on Ethical Hacking and Penetration Testing* (pp. 95-113).

www.irma-international.org/chapter/early-detection-of-security-holes-in-the-network/330261

Ethical Challenges and Innovations in AI-Driven Healthcare and Engineering: A Review of Blockchain, Cybersecurity, Data Privacy, and Knowledge Management

Sunakshi Mehra, Meena Rao, Ankit Vijay Bansal, Nitasha Rathore, Sagar Sidana, Sandeep Raj, Anurag Sinha, G. Madhukar Rao, Rejuwan Shamim, Neetu Singhand Biresh Kumar (2025). *Ethical Dimensions of AI Development* (pp. 323-346).

www.irma-international.org/chapter/ethical-challenges-and-innovations-in-ai-driven-healthcare-and-engineering/359650

Introduction to Ransomware

Qasem Abu Al-Haijaand Noor A. Jebril (2023). *Perspectives on Ethical Hacking and Penetration Testing* (pp. 139-170).

www.irma-international.org/chapter/introduction-to-ransomware/330263

Women to the Rescue in Cyber Space

Kristin Brittainand Marianne Robin Russo (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1177-1188).

www.irma-international.org/chapter/women-to-the-rescue-in-cyber-space/228776

Cyber Resilience for the Internet of Things

Marcus Tanqueand Harry J. Foxwell (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1018-1049).

www.irma-international.org/chapter/cyber-resilience-for-the-internet-of-things/228767