



Fake Identities in Social Cyberspace: From Escapism to Terrorism

Lev Topor, ISGAP, USA & Woolf Institute, University of Cambridge, USA & CCLP, University of Haifa, Israel*

 <https://orcid.org/0000-0002-1836-5150>

Moran Pollack, Bar Ilan University, Israel

 <https://orcid.org/0000-0003-2746-5898>

ABSTRACT

Personation, the act of assuming another's identity with the intent to deceive, is an ancient phenomenon. In this article, the authors seek to research online impersonation and to uncover the causes of this phenomenon. They do so by analyzing and comparing several case studies while referring to more traditional concepts of social identity. As discovered, on the one hand, users can create fake identities to enhance their personalities for personal reasons such as voyeurism or as means of escaping reality, or even promote human rights by avoiding local authoritarian censorship. On the other hand, malicious users like terrorists or criminals manipulate online users with phishing attempts and frauds, making social cyberspace less secure.

KEYWORDS

Cyber Security, Cybercrime, Fake Identity, Fraud, Personation, Phishing, Social Networks, Terrorism

INTRODUCTION

Numerous recent incidents of personations – fake profiles - on social cyber space (SCS) have raised concerns and criticism on the ease with which manipulation and fraud can be made; cyber-safety has become a sought-after concern. Specifically, a concern over the ease of utilizing fake identities for negative causes like terrorism, crime and disinformation (Dodel & Mesch, 2019; Clifford, 2019; UNICRI, 2020). Cyber-safety has grown to be a concern of many technological companies. For instance, *Facebook* has shut down 583 million fake profiles in the first quarter of 2018 since they violated *Facebook's* policies and terms of service (Griffin, 2018). Moreover, according to the October 2020 homeland threat assessment by the Department of Homeland Security (DHS), cyber espionage and cybercrime are among the most probable threats to people in the United States (US) and elsewhere (DHS, 2020).

Interestingly, personation, the act of making and taking a fake identity in order to deceive somebody else is an ancient phenomenon that was used throughout history by writers, critics of the authorities, terrorists and criminals alike. In this article we aim to develop a discussion on the

DOI: 10.4018/IJCWT.295867

*Corresponding Author

implications and usages of this phenomenon in SCS, specifically social network sites and anonymous platforms like dark webs. Our research question is simple – Why web users use fake identities, and what for? Our attempt to answer this question is achieved through a comparative analysis of various selected cases of impersonation alongside a constant comparison to different variations of fake identities, aimed to discover the key types of fake identities. Moreover, as described further on, the fact that we (both authors) were subject to an attempt of information gathering created the motivation to research and analyze this phenomenon.

We discovered that malicious users utilize SCS platforms to commit negative acts such as fraud, identity theft, espionage, terrorism and other manipulations. Those who once deceived innocent people on the busy streets of our cities are currently deceiving innocent people in SCS. However, it is important to mention that the term “fake” is not dichotomous. Currently, a great number of social network users manipulate and enhance certain characteristics of their identities, their profiles, for personal needs such as means of escaping reality or voyeurism, some find love while presenting only the positive facts about themselves while hiding the negative, some even promote human rights while evading local authoritarian censorship by creating fake identities or using privacy platforms such as the dark web. Even though the great and immediate danger is indeed terrorism, crime and fraud, we have discovered that there are some shades of grey within this phenomenon. That is, cases of escapism can truly benefit the ones who fake it – who fake or enhance their personalities. In some cases, it can be difficult to identify how “fake” a profile is, whether it’s shade is too dark or whether its shade is light enough to be considered socially and legally legitimate.

Conceptual Framework: Identity on Social Cyberspace

Identity is defined as a complex structure of personal psychological and extroverted sociological set of characteristics. Psychologically, one’s identity contains objective traits such as the way one acts and more subjective traits such as the way one thinks he acts, how others perceive him and how one wants others to perceive him or how one thinks others perceive him (Elliott, 2019, 1-45; Jenkins, 2014, 1-16; Burke & Stets, 2009, 1-3, 18-32, 61-89). The definition of identity can be expanded and explained in a more extroverted and physical manner – one’s descriptive characteristics. For instance, body structure and shape, facial shape and expressions, height, weight, skin color and tone, hair color, tone and type. Additionally, one’s identity has birth-related characteristics such as age, sex and gender, place of birth, family, friends and relationships and last but certainly not least, the socio-economic environment in which one was born (Suh, 2012).

Identity is a social concept; it is tangled in the broader human circle and public sphere and cannot be separated from various social life-related circumstances. Therefore, identity can even be considered as a type of behavioral strategy, it is culturally influenced, and one can even adapt his/hers identity to his/her target audiences. Moreover, as we later show in our analysis of identity types and fake identities, not only psychological or perception related traits and characteristics can be adapted, concealed or enhanced, but even physical characteristics can be manipulated in SCS. When one enters a social environment, the members of that specific social sphere, the community, constantly seek and examine information about him/her. The community is interested in his/hers physical, psychological and social characteristics such as gender, age or color, language, manners and socio-economic status. This information helps members of the community to define the situation and assess the personality they interact with. Further, community members can even signal or tell other members of what to expect from the mentioned object (Goffman, 1959, 46-75).

With the contemporary age of web and information and the development and proliferation of SCS, physical presence became of less importance and, as we have witnessed worldwide, crises like the Coronavirus pandemic made real world social interactions very limited, masks made it difficult to perceive and understand situations. Social isolation even led to an increase in mortality (Miller, 2020). In the context of this article, perception is a term which was generally related to real social interactions but now SCS platforms redefine the term. The absence of a physical presence and the

15 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/article/fake-identities-social-cyberspace/295867

Related Content

Managing Organized Crime

Roberto Musotto, Davide Di Fatta, Walter Vesperi, Giacomo Morabito, Vittorio D'Aleo and Salvatore Lo Bue (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 1093-1106).

www.irma-international.org/chapter/managing-organized-crime/251481

The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies

Martti Lehto (2013). *International Journal of Cyber Warfare and Terrorism* (pp. 1-18).

www.irma-international.org/article/the-cyberspace-threats-and-cyber-security-objectives-in-the-cyber-security-strategies/104520

Toward a Model for Ethical Cybersecurity Leadership

Marisa Cleveland and Tonia Spangler (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 294-302).

www.irma-international.org/chapter/toward-a-model-for-ethical-cybersecurity-leadership/251433

How Can World Leaders Understand the Perverse Core of Terrorism?: Terror in the Global Village

Maximiliano E. Korstanje (2019). *Violent Extremism: Breakthroughs in Research and Practice* (pp. 188-202).

www.irma-international.org/chapter/how-can-world-leaders-understand-the-perverse-core-of-terrorism/213306

All Hazards Analysis: A Complexity Perspective

Daryl Essam and Hussein A. Abbass (2006). *Applications of Information Systems to Homeland Security and Defense* (pp. 1-16).

www.irma-international.org/chapter/all-hazards-analysis/5144