CALL FOR PAPERS – SPECIAL ISSUE JOURNAL OF THE MIDWEST ASSOCIATION FOR INFORMATION SYSTEMS (JMWAIS)

THEME: INFORMATION SECURITY AND PRIVACY - THE CHALLENGE OF NEW TECHNOLOGIES

Description:

The recent proliferation of new information technologies such as artificial intelligence/machine learning, the Internet of Things (IoT), cryptocurrencies, blockchain and cloud storage and computing have created new challenges for advocates of information security and privacy. Traditional controls such as demilitarized zones, intrusion detection systems, patch management systems, and firewalls may not be sufficient to protect data, systems, and privacy. Existing research extolls the benefits of these new technologies in a variety of scenarios and contexts. Smart home automation can be beneficial to the handicapped and elderly. Home security camera can protect property and belongings, and have even been used to help law enforcement solve crimes. Wearable technologies like smart watches with ECG technology can warn users when a serious health issue may be present. Other new technologies like cryptocurrencies (e.g. Bitcoin) and cloud computing promise new opportunities for business and commerce.

However, research to date has yet to consider the security and privacy implications of these promising new technologies. For example, recent news reports of major data breach in fitness-tracking apps (Dickey 2018) and wearable devices data compromising the location of secret military bases (Taylor 2018) underscore the security consequences and instigate a lack of trust. It has been reported that an AI algorithm lead to the erroneous firing of teachers (Thomas 2019). In another report, a company AI human resource recruiting initiative concluded that all female applicants were unacceptable for corporate leadership positions (Harrer 2018). In other cases, home security camera that are easy for users to install are also easy for hackers to exploit. Along with the security implications are the privacy issues. Wearables and other IoT devices enable the collection of vast amounts of data involving millions of people. Users need to understand these privacy implications in order to make informed choices with respect to the devices used and configured. This special issue calls for research papers that investigate the information security and privacy challenges that accompany the new generation of technologies.

We seek completed research papers in topics including but not limited to:

- Privacy and Security risks posed by home automation on personal data.
- Proliferation of security risks posed by home automation to organizations.
- Future of cyber-crime and cyber-terrorism in the age of ubiquitous technologies.
- Privacy and Security risks posed by wearables on personal health information.
- Policy considerations for new technologies such as IoT.
- Privacy and Security risks posed by cryptocurrencies on financial information.
- Policy considerations for cryptocurrencies.
- Implications of sharing economy on information privacy and security.
- Feasibility of expansion of existing security controls to IoT.
- Privacy and Security standards in IoT-enabled devices that contain cameras and microphones.
- Ownership and Informed consent of information generated by IoT and Ubiquitous technologies
- Security Implications of novel financial technologies (FinTech) including mobile payments and blockchain.
- Security considerations for cloud computing and storage.
- Cloud storage security configurations.
- Legal and contractual issues in cloud storage.
- Security implications when aggregating large data sets for analytics.
- Public knowledge and perceptions of artificial intelligence.
- Ethical issues of artificial intelligence and machine learning.
- Risks and mitigation strategies for artificial intelligence and machine learning.
- Unintended consequence of artificial intelligence and machine learning.

References

Dickey, M. R. 2018. "Under Armour Says Myfitnesspal Data Breach Affected 150 Million Users." from https://techcrunch.com/2018/03/29/under-armour-says-myfitnesspal-data-breach-affected-150-million-users/ Last accessed July 24, 2019

Harrer, A. 2018. "Amazon Scraps a Secret A.I. Recruiting Tool That Showed Bias against Women," from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G Last accessed July 24, 2019

Taylor, G. L. a. R. 2018. "Pentagon Reviewing Troops' Use of Fitness Trackers in Light of Security Concerns," in: *The Wall Street Journal*. Washington D.C.

Thomas, R. 2019. "Five Things That Scare Me About Ai." from https://www.fast.ai/2019/01/29/five-scary-things/ Last accessed July 24, 2019

Important Dates:

Date	Event
January 15, 2020	Deadline for manuscript submission: by midnight PST
March 15, 2020	First round reviews sent to authors
April 15, 2020	Submission of requested revisions
April 30, 2020	Authors notified of final publication decision
May 31, 2020	For accepted articles, camera ready article for publication due by midnight PST for final editorial review
July 2020	Publication in Journal of the Midwest Association for Information Systems (JMWAIS)

Submitted papers should adhere to JWMAIS submission guidelines. Submit papers to: David Biros (david.biros@okstate.edu). Please use email title "SI-Security and Privacy"

For further information contact the Special Issue Editor David Biros, Management Science and Information Systems, Oklahoma State University (david.biros@okstate.edu).

Guest Editor Information

David P. Biros, PhD (Lt Col, USAF Retired)
Associate Professor of Management Science
and Information Systems
Fleming Chair in Technology Management
MSIS PhD Program Chair
Oklahoma State Univeristiy
david.biros@okstate.edu
Office (405) 744-7156 Fax (405) 744-5180