Journal of the Midwest Association for Information Systems

Volume 2020 | Issue 2 Article 1

Editor's Comments

Date: 07-31-2020

The Challenges of New Information Technology on Security, Privacy and Ethics

David P. Biros
Oklahoma State University, andyluse@okstate.edu

Abstract

The rapid rate of growth and change in Information technology continues to be a challenge for those in the information sector. New technologies such as the Internet of Things (IoT) and wearables, big data analytics, and artificial intelligence (AI) are developing so rapidly that information security and privacy professionals are struggling to keep up. Government and industry call for more cybersecurity professionals and the news media make it clear that the number of cybersecurity breaches and incidents continues to rise. This short article exams some of the challenges with the new technologies and how they are vulnerable to exploitation. In order to keep pace, information security education, ethics, governance and privacy controls must adapt. Unfortunately, as history shows us, they are slow to evolve, much slower than the technologies we hope to secure. The 2020s will usher in vast advancements in technology. More attention needs to be given to anticipating the vulnerabilities associated with that technology and the strategies for mitigating them.

Keywords: Internet of Things (IoT), big data analytics, Artificial Intelligence (AI), security ethics, privacy, risk

DOI: 10.17705/3jmwa.000057

1. Introduction

I have been working in information security for nearly 30 years. In the fall of 1991, I was a young Captain in the US Air Force and just beginning a Master's degree program in Information Resource Management at the Air Force Institute of Technology (AFIT). I had just purchased a new PC with a whopping 1 MB RAM and a 40 MB hard drive and was setting it up to connect to AFIT with my 2400 baud modem, when a friend called to tell me about a computer virus going around. He said it was called the Michelangelo virus and it affected master boot record of your computer if it was infected. The virus would activate on Michelangelo's birthday (March 6). It was then that I decided to learn more about information security or as we called it in the military, information assurance. Over the years, I was part of a military information security inspection (audit) team, served a DoD task force for complying with the Federal Information Security Management Act (FISMA, 2020), drafted Air Force information assurance policy, served as the Chief Information Security Officer (CISO) for the Air Force CIO, taught dozens of information security and risk assessment coursed, and researched and published articles on security vulnerabilities.

One thing is certain. The domains of information security and privacy are evolving and doing so rapidly. Technologies are changing and more data is being collected than ever before. We used to count viruses in the thousands. Now we count them in the millions. We used to connect to the Internet with a home computer using dial-up connections for a limited period of time. Now everything connects to the Internet all the time (i.e. Internet of Things). Data storage used to be expensive, relatively speaking, and policy makers and developers limited how much data was collected and how many lines of code were written. Now, there is more data collected than ever before and that data is used in ways never imagined (big data analytics, training artificial intelligence).

Yet with all the advances in technology, our information security risk continues to grow. Everything connected to the Internet is a potential target and, in turn, a security vulnerability. Extremely large data sets hold massive amounts of sensitive and valuable information that are vulnerable to loss. Artificial Intelligence (AI) is poised to change the world again but has its own vulnerabilities (Biros, et al., 2019). Not only that, there are also implications for privacy, ethics, and education both at home and in the workplace. Fortunately, the authors of the papers in this special issue (introduced later) have done a great job at investigating the changes to these all-important facets of information security. First, a closer look at the aforementioned technologies is in order.

2. Rapid Growth of IoT and Wearables

Probably the greatest source of new information security vulnerabilities and loss of privacy is with IoT and wearables. Oberländer et al (2018), define IoT as "connectivity of physical objects equipped with sensors and actuators to the internet via data communication technologies." We have smart speakers, doorbells with cameras connected to our wifi; smart watches to tell us how much to walk and how well we slept; autonomous vehicles, and AI systems that monitor our driving, vet applicants for jobs, and prevent us from jaywalking (Sharma and Biros, 2019; Biros, et al, 2019). Further, as two of our authors in this issue note, businesses also use IoT for performance monitoring. In many cases, it is not the technology itself, but the user's inability to properly configure either the device or their home wifi system. While some earlier, high-profile attacks were directed toward Internet cameras and baby monitors (Wang 2018), in 2019 information security breaches due to IoT devices as starting point for deeper networking hacks became a major concern (Buntz, 2019). In short, the addition of IoT to our world has led to millions of new targets to be exploited.

A major subset of the IoT is wearables or internet connected devices that can be incorporated into clothing or worn as an accessory. Apple watch and Fitbit devices are common examples. They have the ability to monitor heart rate, calories burned, steps or mile walked or ran, and sleep patterns and quality. Most often the devices are paired with apps that collect and analyze the data before reporting results back to their owners. It is estimated that by next year 378.8 million devices will be in use in the US alone. (Statista 2019). As noted, the data is collected and analyzed for pre-defined purposes, but it can also have unintended consequences. This is not to say wearable are bad. On the contrary, there are a number of reports of wearables alerting users of previously undiagnosed and potentially fatal heart conditions (Reisinger 2018), however there have been serious cases of wearable data used for purposes that the manufacturer never intended. In a recent report, military troops using wearables and a fitness-oriented social networking app that track users running routes compromised the locations of some secret US military bases (Miller 2018). According to Hsu (2018), a popular fitness app company, Strava, used heat maps to graphically represent the locations of runners and others

exercising. While it was expected that densely populated areas would show high heat, some areas thought to be uninhabited depicted patterns of heat. In turn, these areas were correctly surmised to be secret military bases in remote parts of the world. The massive amounts of data generated by IoT and wearables can be analyzed for both positive and negative purposes.

3. Big Data Analytics

IoT and wearables make up only part of the data collection picture. All toll, in 2018, about 2.5 quintillion bytes of data were created every day (Marr 2018). This included data produced by Internet searches, social media, communications, digital photos, services, and IoT and wearables. All of this data is analyzed to produce meaningful information impacting many areas of society (Gupta, et al., 2018). It has been used in health care, firm performance, society activities and more. Big data analytics can help diagnose medical conditions, analyze comorbidities in health care, and help to optimize traffic flow.

With all the potential capability some very serious concerns remain, one of them being privacy implications (Jenson, 2013). Almost anyone who has ever used Amazon knows it targets individual customers based on their purchasing history. Searches on Google result in advertisements that reflect the subject of a recent search. All of the data collected can be sold or transferred without the consumer's knowledge or consent (or awareness of consent). The world of big data analytics continues to eat way at the privacy rights of individuals. While there are some laws such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018, there continues to be significant privacy challenges and implications. In some cases, such as AI, even developers and analysts do not fully understand how the data will be used and interpreted.

4. Artificial Intelligence

Another technology worth noting is AI. It is a rapidly going field with many applications. Organizations are using AI to help select potential employees, build autonomously driving cars, monitor prescription drug doses and prevent credit card fraud (Biros, et al., 2019). AI tools are trained by very large data sets to recognized patterns and trends and act on them. It has the potential to reduce production costs, cut time to accomplish tasks (e.g. sifting through thousands of resumes) and help enforce laws and statutes. The technology requires big data to adequately train systems that use decision trees, neural networks and other advancements to make decisions on behalf of human decision makers.

Like the other technologies mentioned AI has its challenges as well. As Biros and colleagues (2019) demonstrated, AI projects suffer from problem fit, input data issues, and application problems. For example, Amazon created a recruiting tool to help it recruit and hire more women. However, the data used to train the tool came from the previous ten years of resumes from male-dominated tech companies. As a result, the tool showed a bias against women. In Ningbo, China an AI application designed to catch jaywalkers erroneously cited a well-known business woman for jaywalking because her picture was on the side of bus in the street (problem fit). Also, a company is Israel developed a face recognition program they claimed could identify pedophiles and terrorists by analyzing their physical traits. Multiple scientists have questioned the validity of the tool and the ethical implications enormous. If such technology gets into the wrong hands or if it should be hacked and manipulated, the results could be disastrous.

5. Summary and Recommendations

The three major technologies mentioned above have the potential to help us live longer and healthier lives, understand more about health care issues and production optimization, and reduce the number of tedious tasks we must perform. However, we cannot overlook the potential they have for security, privacy and ethical implications that come with them. They bring with them vulnerabilities of too much data sharing, aggregating massive amounts of data in one location, and lulling us into relying on them for all of decision-making tasks. It is important that we investigate the privacy concerns and ethical consideration of such technology. Fortunately, the papers included in this special issue do just that.

6. Overview of the contents of this issue

This issue contains four articles on information security, privacy and ethics.

Luse, A and Burkman J. investigate the use of RFID wearables in the context of a corporate environment using privacy boundary research. Their findings show that while being monitored negatively impacts employee satisfaction, greater

transparency in implementation may alleviate some of the negative aspects of implanting such technologies in the workplace.

Young J., Smith T., and Zheng, S. extend Mason's information ethics framework of privacy, accuracy, property and accessibility (PAPA) to capture some of today's new technology considerations focused around big data. Their extension includes the concepts of behavioral surveillance, governance and privacy.

Maunula, G. demonstrates that the analysis of sharing economy processing activities uncovers potential privacy, security and data protection concerns related to a platform's disclosure of personal data to end-users. This has considerable implications for compliance with the GDPR and she posit that is correction requires a multi-disciplinary approach.

Weiser M. and Bowman A. round out the articles with a content analysis of the leading information security textbooks as compared to the needs of employers with respect to the skillset of the university graduates. The results of study found that coverage of terms associated with security knowledge areas demanded by the marketplace requires attention if schools are going to turn out well qualified information security knowledgeable graduates.

7. References

Biros, D., Sharma, M., and Biros, J., (2019) Vulnerability and risk mitigation in AI and machine learning" *Cutter Business Technology Journal*, 32 (8)

Buntz, B. (2019) A year in review: 12 IoT security considerations. *IoT World Today*, Retrieved from. https://www.iotworldtoday.com/2019/08/15/a-year-in-review-12-iot-security-considerations/

Gupta, A., Deokar, A., Iyer, L. et al. (2018) Big data and analytics for societal impact: Recent research and trends. *Information Systems Frontiers*, 20**,** 185–194.

Hsu, J. (2018) The Strava heat map and the end of secrets. *Wired*. Retrieved from https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

Jensen M. (2013) Challenges of privacy protection in big data analytics, *2013 IEEE International Congress on Big Data*, pp. 235-238

Marr, B. (2018) How much data do we create every day? The amazing stats everyone should know. *Forbes.* Retrieved from https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#7fa5414360ba

Oberländer, A. M., Röglinger, M., Rosemann, M., and Kees, A. J. E. J. o. I. S. (2018). Conceptualizing business-to thing interactions–a aociomaterial perspective on the Internet of Things," (27:4), pp. 486-502.

Reisinger, D. (2018). Apple Watch Credited with Saving a Man's Life." Fortune. Retrieved from http://fortune.com/2018/05/03/applewatch-saves-life/

Sharma M. and Biros, D. (2019) Building trust in wearables for health behavior *Journal of the Midwest Association of Information Systems*, (2019:2)

Statista (2019). Wearable device unit sales worldwide by region from 2015 to 2021 (in Millions). Retrieved from https://www.statista.com/statistics/490231/wearable-devices-worldwide-by-region/

Taylor, G. L (2018). Pentagon reviewing troops' use of fitness trackers in light of security concerns, *The Wall Street Journal*.

Wang, A. (2018) I'm in your baby's room: A hacker took over a baby monitor and broadcast threats, parent say" *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/

Author Biography

Dr. David Biros is an Associate Professor of Management Science and Information Systems and Fleming Chair of Information Technology Management at Oklahoma State University. A retired Lieutenant Colonel of the United States Air Force, Dr. Biros' last assignment was as Chief, Information Assurance Officer for the AF-CIO. His research interests included deception detection, insider threat, information system trust and ethics in information technology. He has been published MIS Quarterly, the Journal of Management Information Systems, Decision Support Systems, Group Decision and Negotiation, MISQ Executive, the Journal of Digital Forensics Security and Law and other journals and conference proceedings.

This page intentionally left blank