THE QUALITY OF DIGITIZED DATA IN A CRITICAL DECISION-MAKING CONTEXT

Kristen L. Walker, Nazarian College of Business & Economics, California State University Northridge, 18111 Nordhoff St., Northridge, CA 91330, 818-677-2040, kristen.walker@csun.edu
Mary Curren, Nazarian College of Business & Economics, California State University Northridge, 18111 Nordhoff St., Northridge, CA 91330, 818-677-2458, mary.curren@csun.edu
Tina Kiesler, Nazarian College of Business & Economics, California State University Northridge, 18111 Nordhoff St., Northridge, CA 91330, 818-677-4608, tina.kiesler@csun.edu

EXTENDED ABSTRACT

In this age of the Internet of Things (IoT), information is exchanged among many sources, sometimes directly from consumers via home and office technologies and sometimes from other government and industry sources as well as third-party data-management firms. The Internet of Things creates data streaming from home devices and technology such as smart phones and smart TVs, wearables such as exercise monitors, search engines, RFID, social media sites, municipal cameras/CCTV) and more.

In today's data-driven marketplace, with increasing collection and exchange of consumer information, what measures are firms using to protect the privacy of data sources and the exchanges of their information online? Not only is privacy protection an issue, but how *accurate* is the information being exchanged? Issues of privacy and security are top of mind in our informational era, reliant on transparency and trust among parties. The accuracy of these data sources is critical since they are key resources for many industries. Firms such as databrokers, security and protection services, government agencies, and marketers use these data as inputs for the algorithms that produce more information.

Firms are struggling to manage these exchanges of information. In early May 2017 Facebook announced they were improving technology to detect inappropriate content and they planned to hire 3,000 more employees in roles as "moderators" to "speed up" the review of content flagged or reported by users (Kuchler, 2017). Firms and consumers are moving to "deliver integrated, real-time, relevant experiences" (Stephen and Lamberton, 2016). "Stories" and "live" options are available on most social media applications, meaning that larger packages of digitized information are continuously produced and accessible.

In our exploratory study, we examine these issues in an industry particularly impacted by the need for accurate information acquired quickly—the security and protection industry. Since security and protection rely on the need for accurate information to reduce risk and protect assets, research in this industry provides valuable insight into how organizations rely on data for critical decisions. From what sources do they acquire data? To what extent do they question and verify the accuracy of the data and its purity? We conducted surveys and interviews with experts in the security and protection industry, across several organizations, to determine how these organizations assess the quality of information they receive for security and protection-related decisions. *If* quality is assessed, to what extent is it verified by humans and to what extent by technology? How do organizations manage the tradeoffs between the need for quick information to make fast decisions in security and protection contexts and the need for

accurate information, if it is perceived as a tradeoff at all? How do they manage the desire to trust the sources of the information with their need to verify its accuracy?

In the first part of our study, we interviewed the key players acting as intermediaries of data for command centers. Since this is a relatively new form of intermediary, these firms are currently few in number, yet emerging. Thus, we interviewed the top 5 security and protection companies in this area to learn about the sources used by their command centers. We discussed the number of sources and the processes they used to verify data accuracy as well as the role of staff members (and their certification requirements) in the verification process. We then surveyed representatives of security and protection organizations about their data suppliers by approaching them at a security industry conference. Representatives answered questions (on seven-point scales) about the extensiveness of procedures their organization has in place for monitoring information sources, their perceived trustworthiness of those data sources, the importance of the data vendors to the security organization (relative to other types of vendors), perceived switching costs, and challenges associated with working with vendors who serve as sources of data.

Preliminary results indicate security and protection organizations are indeed handling large amounts of data and they are using it with very little human intervention to verify accuracy. This finding alone has important implications for the meaningfulness of decisions organizations make based on data from citizens, technology, and third parties.

References available upon request from the authors.