"Truth Machines" from Polygraphs to Neural Analysis: Technologically-Assisted Cheating and Deception Detection in Historical Focus

Abstract

Cheating and deception are often construed as having considerable social and economic consequences in critical social contexts such as workplaces and immigration settings (Jacobsen, Fosgaard, & Pascual-Ezama, 2018). Discourses on truth and falsity have increased in number and variety as many commentators have characterized our society as being in a "post-truth" era (Oravec, 2018; Peters, Rider, Hyvönen, & Besley, 2018). Developing a set of technological tools to assist in detection of "lies," "cheating," and "false impersonation" (however murky and confusing these notions can be) has long been an aspiration of some developers and managers, with the dreams and visions of creating a "truth machine" still active (Gaggioli, 2018). The concepts of truthfulness and deception as implemented in online systems by researchers and technicians can be significantly different from the notions that are embedded in everyday organizational understandings and enactments. The paper begins by exploring the history of polygraphs. It then examines the construction and labelling of online "integrity scores"; it investigates how such vehicles as wearable technologies, eye scanning, and webcams are being used to collect the data used for anti-deception initiatives (as with Converus's EyeDetect), along with the increasing levels of personalization of deception prevention (Whelan, McDuff, Gleasure, & Vom Brocke, 2018). The paper projects the dangers of organizations and governmental agencies producing "lists of potential cheaters" linked with detailed profiles and composed of names of individuals whose recorded movements and characteristics apparently do not conform to the behavioral indicators projected by particular systems. The paper also outlines some of the future prospects for brain scanning and other emerging modes for deception detection as well as behavioral modification; the notion of "self-lie detection" has been investigated by researchers, with the projected potential for increasing personal insight about one's own truthfulness through technological means (Echarte, 2019).

Use of polygraphs on employees is often prohibited or constrained in many US and international business contexts (Balmer, 2018); however, some forms of "virtual polygraphy" (Schrage, 2011) have emerged that have not been explicitly banned in many of their implementations. Despite many technical and legal obstacles, new capabilities for detecting lies, deception, and false impersonation have been integrated into various technological systems, increasing the "personal transparency" of employees and often of clients as well (Han, 2015; Oravec, 2004; Warren & Schweitzer, 2018). Some of these

deception-detection mechanisms capture employee documents, profiles, and personal characteristics and behaviors for later use in system analytics or in other applications, possibly presenting privacy invasions. Informing employees about the systems' intents and requesting consent about deception detection has the potential to challenge some individuals to "game" the systems and attempt to subvert the detection mechanisms involved (Oravec, 2013). This essay analyzes the efforts of ProctorU, Converus (EyeDetect), and Examity Corporations, and extends the discussion to the robotic detection of deception (Iacob & Tapus, 2018). (ProctorU and Examity initiatives were once primarily focused on student cheating, but have expanded in applications to workplace settings.) Issues of whether the full intent of the systems can be communicated in a comprehensible fashion are of special concern in efforts to obtain informed consent and to implement the systems humanely.

Big data, profiling, surveillance, and predictive analytics in deception detection systems may change radically the relationships between individuals and organizations, introducing new potentials for bias and disempowerment. Research and development efforts on cheating and deception have gained new dimensions in the advent of artificial intelligence (AI) and big data capabilities, and some of the resultant initiatives are in use today despite the fact that they are in the early stages of testing and evaluation.

Some references:

Balmer, A. (2018). *Lie detection and the law: Torture, technology and truth*. New York: Routledge.

Bryant, P. (2018, December 21). Will eye scanning technology replace the polygraph. *Government Technology*. Retrieved from http://www.govtech.com/public-safety/Will-Eye-Scanning-Technology-Replace-the-Polygraph.html

Echarte, L. E. (2019). Self-lie detection: New challenges for moral neuroenhancement. In *Psychiatry and Neuroscience Update* (pp. 43-52). Springer, Cham.

Gaggioli, A. (2018). Beyond the Truth Machine: Emerging Technologies for Lie Detection. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 144-144.

Han, B. C. (2015). *The transparency society*. Stanford University Press.

Iacob, D. O., & Tapus, A. (2018, August). First attempts in deception detection in HRI by using thermal and RGB-D cameras. In *2018 27th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)* (pp. 652-658). New York: IEEE Press. Retrieved from https://ieeexplore.ieee.org/document/8525573

Jacobsen, C., Fosgaard, T. R., & Pascual-Ezama, D. (2018). Why do we lie? A practical guide to the dishonesty literature. *Journal of Economic Surveys*, *32*(2), 357-387.

Llewellyn, N., & Whittle, A. (2018). Lies, defeasibility and morality-in-action: The interactional architecture of false claims in sales, telemarketing and debt collection work. *Human Relations*, 0018726718778093.

Oravec, J. A. (2004). The transparent knowledge worker: Weblogs and reputation mechanisms in KM systems. *International Journal of Technology Management*, *28*(7-8), 767-775.

Oravec, J. A. (2013). Gaming Google: Some ethical issues involving online reputation management. *Journal of Business Ethics Education*, *10*, 61-81.

Oravec, J. A. (2017). The manipulation of scholarly rating and measurement systems: Constructing excellence in an era of academic stardom. *Teaching in Higher Education*, *22*(4), 423-436.

Oravec, J. A. (2018). Secrecy in educational practices: Enacting nested black boxes in cheating and deception detection systems. *Secrecy and Society*, *1*(2), 5.

Orlando, J., Hanham, J., & Ullman, J. (2018). Exploring intentional use of a technological proxy, Turnitin, to enhance student academic literacy practices. *Australasian Journal of Educational Technology*, *34*(4), 44-56.

Peters, M. A., Rider, S., Hyvönen, M., & Besley, T. (Eds.). (2018). *Post-truth, fake news: Viral modernity & higher education*. Springer.

Schrage, M. (2011). The future of lie detection in the workplace. *Harvard Business Review*. Retrieved from https://hbr.org/2011/08/most-managers-wouldnt-dream-of.html

Warren, D. E., & Schweitzer, M. E. (2018). When lying does not pay: How experts detect insurance fraud. *Journal of Business Ethics*, *150*(3), 711-726.

Wertheim, E. G. (2016). The truth about lying: What should we teach about lying and deception in negotiations: An experiential approach. *Business Education Innovation Journal*, *8*(2).

Whelan, E., McDuff, D., Gleasure, R., & Vom Brocke, J. (2018). How emotion-sensing technology can reshape the workplace. *MIT Sloan Management Review*, *59*(3), 7-10.