Katherine Pratt

WeRobot 2019 Poster Description

The video of a robot doing parkour (Atlas, Boston Dynamics) provokes an instinctive fear of Terminator-like androids coming to overthrow humanity. But one need only watch the blooper reel from DARPA's Robotics Challenge to understand how far away we really are. Human control of robots and other physical and digital devices will continue to be much more mainstream (at least until Data becomes a reality). Therefore, novel modalities for controlling things as varied as a telepresence robot or smartphone is an area of increased interest, as researchers and industry innovate methods to make such control as seamless and intuitive as possible.

One method may come straight from the brain, by recording neural signals and using that information to control a device separate from the body: a brain-computer interface (BCI). There is a novelty in playing a videogame by simply putting on a hat with embedded electrodes, or controlling a prosthetic arm like Luke Skywalker, but such innovation hides deep ethical and policy questions about commercial access to and use of neural signals.

Neural signals that are recorded under the auspices of medical care or research are covered in the US by HIPAA or consent form approved by an institutional research board, respectively. But what happens when it is a commercial entity that is recording the neural signals? Startups and tech billionaires alike are researching how to commercialize BCIs, thus creating a grey area of who "owns" someone's neural signals and the information derived from them. Researchers have already demonstrated the feasibility of using neural signals to elicit everything from month of birth to a 4-digit PIN number [1][4][5][6]; the risks and potential responses (such as a BCI anonymizer) are also published [2][3]. One of the biggest challenges in the field is the quantitative uncertainty of the risk to consumers, both with current technology and extrapolated future capabilities.

Concurrent with this quantitative work are questions involving ethics and policy; if potential consumers learn about the possibility that private information can be derived neurally, there may be greater grievance. Thus, it is not an objection to the information that is compromised, but a foreign entity interpreting an individual's neural signals. The opinions of potential users may help to drive the minimum regulations or protections that are desired for neurally-controlled devices. This tie between ethics and policy represents a novel but necessary area of discussion that should become commonplace for all emerging technologies.

This poster will discuss the preliminary findings of dissertation work that addresses the questions of using neural signals to elicit private information, how potential consumers perceive this risk, and policy approaches to protect neural signals. Additionally, it will suggest a model framework for others to apply to mutidisciplinary engineering research projects.

Selected Sources Cited

[1] T. Bonaci, Dissertation: "Security and Privacy of Biomedical Cyber-Physical Systems," 2015.

[2] T. Bonaci, R. Calo, and H. J. Chizeck, "App stores for the brain: Privacy amp; security in Brain-Computer Interfaces," in *2014 IEEE International Symposium on Ethics in Science, Technology and Engineering*, 2014, pp. 1–7.

[3] H. J. Chizeck and T. Bonaci, Patent: *Brain-Computer Interface Anonymizer*. 2014.

[4] M. Frank *et al.*, "Subliminal Probing for Private Information via EEG-Based BCI Devices," *arXiv:1312.6052 [cs]*, Dec. 2013.

[5] J. Lange, C. Massart, A. Mouraux, and F.-X. Standaert, "Side-Channel Attacks Against the Human Brain: The PIN Code Case Study," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*, 2017, pp. 171–189.

[6] I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, and D. Song, "On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces," presented at the Presented as part of the 21st USENIX Security Symposium (USENIX Security 12), 2012, pp. 143–158.