Proceedings of the World Congress on Electrical Engineering and Computer Systems and Science (EECSS 2015)
Barcelona, Spain – July 13 - 14, 2015
Paper No. 311

Hacking the Brain: Neurosecurity Issues from an Ethical and Legal Perspective

Marcello Ienca
Institute of Biomedical Ethics, University of Basel
Bernoullistrasse 28, Basel, Switzerland
marcello.ienca@unibas.ch

Extended Abstract

Brain-computers interfacing (BCI) technologies are being increasingly used as assistive technologies for several classes of neurological patients as well as everyday technologies for healthy people to allow users to control computer devices only by brain activity. BCI applications have the potential of significantly improving life quality in patients (e.g. patients suffering severe neuromuscular disorders) and enabling enhanced and more personalized user experience in communication, gaming and entertainment for general users. Yet the risks associated with the misuse of these technologies by agents for nefarious purposes remain largely unexplored. Recent findings have shown that BCIs can be potentially co-opted for malicious activities such as detecting concealed autobiographical information from users (Rosenfeld, 2011) and extracting sensitive information about the users such as their pin codes, bank membership, and home location without the user's consent (Martinovic et al., 2012). In addition, real-life trials such as the Cody's Emokit project have shown that it is possible to crack encrypted data from a consumer-grade BCI headset (Conner, 2010). These findings open the prospects of extending the range of computer-crime to neural computation. This emerging breach for information insecurity can be labeled as *neurocrime* since it enables criminal activities which target neural information (Denning, Matsuoka, & Kohno, 2009).

The objectives of this paper are twofold. First, at the conceptual level, we aim to define the emerging phenomenon of neurocrime and identify a special type of neurocrime which we called "brain-hacking". We believe this form of neurocrime is critical as it involves the direct access to and manipulation of the informational content of neural computation. The possibility of brain-hacking raises unprecedented issues in information security and content protection as it targets a highly sensitive type of information, i.e. neural information, and accesses or manipulates informational contents ─such as thoughts, beliefs and desires─ that are constitutive of someone's psychological integrity and self-identification as persons. Consequently, this paper will closely examine the implications of neurocrime and brain-hacking for information security and content protection. Second, at the normative level, we address the major ethical and legal implications associated with the potential misuse of BCIs and other forms of neurocrime. We identify significant implications for the moral principles of autonomy, agency, moral responsibility, and personal identity; also, we recognize critical implications for the legal principles of privacy, confidentiality and legal liability. By focusing on neurosecurity issues from an ethico-legal perspective early, we hope to prevent that the deployment of BCIs and other neural devices might be tempered by defective legal or regulatory coverage and might provoke rapid increases in offenses.

This contribution is aimed at raising awareness on the security risks associated with the emerging phenomenon of neurocrime, and takes a first step in developing an ethical, legal, social and regulatory framework to maximize the deployment of BCI technology while minimizing the risks of neurocrime.

Conner, M. (2010). Hacking the brain: Brain-to-computer interface hardware moves from the realm of research. *EDN*, *55*(22), 30-35.

Denning, T., Matsuoka, Y., & Kohno, T. (2009). Neurosecurity: security and privacy for neural devices. *Neurosurgical focus, 27*(1), E7.

Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., & Song, D. (2012). *On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces*. Paper presented at the USENIX Security Symposium.

Rosenfeld, J. P. (2011). P300 in detecting concealed information. *Memory detection: Theory and application of the Concealed Information Test*, 63-89.