Viewpoint

Neuroprivacy, neurosecurity and brain-hacking: Emerging issues in neural engineering

Marcello Ienca[a]

a Research assistant at the Institute for Biomedical Ethics, University of Basel

Nearly one in six of the world population suffers from neurological disorders. Disorders of the nervous system, from Alzheimer's and other dementias, Parkinson disease, multiple sclerosis and epilepsy to strokes, brain and spinal cord injuries, affect people in all countries, irrespective of sex, education or income. The global prevalence of neurological disorders poses a major problem for public health and the health-care services in terms of care provision, caregiving burden and financial management. Availability of appropriate care is frequently constrained by the effectiveness and limitations of present neuropharmacological treatments, and the non-integration of neurological care into primary care. Informal caregivers who assist chronically disabled neurological patients are reported to face a major physical, psychological and financial burden. Health-care systems face correspondingly high economic costs. These include not only the cost of treatment, but also the lost productivity of patients and their caregivers.

A promising approach in response to this global crisis is the development and deployment of cutting-edge neural engineering devices for the treatment, rehabilitation and assistance of neurological patients. With the current capability in microtechnology and computational neuroscience, there is the opportunity to develop devices that can effectively establish a connection pathway between the human nervous system and interfaced electromechanical systems. Brain-controlled computer systems, robotic limbs, neuroprostheses, brain-stimulators, cognitive orthotics, memory aids, hearing and visual implants, are no longer domain of science fiction; they are already commercialized medical technologies or well-corroborated research prototypes. These devices could provide a triple-win effect as they could: (i) provide more rapid and effective treatment, rehabilitation and assistance, thus improving the quality of life of patients; (ii) reduce caregiving burden; (iii) save significant costs to the healthcare system. While neural engineering can have a groundbreaking impact on neurological care and radically improve the quality of life of neurological patients, it raises the issues of dual-use and information security. The reason for that stems from the fact that neural devices, similarly as personal computers, are potentially vulnerable to be manipulated by malicious actors for nefarious purposes. This emerging breach for information insecurity can be labeled as *neurocrime* since it enables criminal activities which target neural information.

Neurosecurity

In order to establish a communication pathway with the nervous system, neural devices such as brain stimulators and brain-computer interfaces are designed to allow computer systems to access and process neural computation. While the accessibility of neural information is crucial for the effective functioning of the device, this feature raises the issue of privacy and information security, as neural information is carrier of private and sensitive data whose access or manipulation by malicious actors may cause significant physical (including life-threatening), psychological or social harm to technology users. With the rapid increase in distribution of neural devices it is expected that neural information will irrigate the digital ecosystem from innumerable sources with an unprecedented quantity of data flows and at an unprecedented velocity. Neural implants for clinical patients, at-home neurostimulators for cognitive enhancement, brain-computer interfacing applications for smartphone and a myriad of other devices are becoming access points of neural information, often connected to the internet. This will also multiply the quantity of data and the number and type of devices that are potentially exposed to security risks.

Brain-Hacking

Neurocrime can target neural information either indirectly or directly. Indirect crime is when the attack is aimed at limiting, modifying or disrupting function in the devices that interface brain information – with neural computation from the users' brain not being accessed or manipulated in any significant sense. This type of risk is already critical at the current level of deployment of neural engineering technologies. With neurally controlled devices (e.g. brain stimulators and brain-computer interfaces) being available as medical technologies as well as commercialized products, present neurocriminals may abuse of the users by disrupting or terminating function in their devices without the users' permission or consent. For example, already commercialized brain-computer interfacing headsets for smartphones could be mechanically destroyed by malicious actors. Direct crime is when the attack cracks the users' neural computation to access and/or manipulate neural information for criminal purposes. I call this special type of neurocrime *"brain-cracking"* or *"brain-hacking"* as it exploits the neural device to get illicit access to and eventually manipulate information in a manner that resembles how computers are hacked or cracked in computer crime. Some forms of brain-hacking have proven to be actually feasible in experimental setting. Studies have shown that brain-computer interfaces can be coopted to detect concealed autobiographical information from users with a significantly high accuracy rate [1]. Even more strikingly, private and sensitive information about the users such as their pin codes, bank membership, and home location was successfully revealed by cracking already commercialized brain-computer interfacing headsets [2]. In addition, first proto-examples of brain-hacking have been also reported outside the experimental setting. A striking case is the so-called Cody's Emokit project through which the hacker Cody Brocious managed to crack encrypted data directly from a consumer-grade brain-computer interfacing headset [3]. A sci-fi future where people can access and manipulate information in other people's brains is approaching at a very high speed and their prodromes are already here. Therefore, all direct and indirect implications of this emerging trend should be urgently assessed.

The dual-use dilemma of neural engineering

The peculiar dual-use dilemma of neural engineering can be summarized as follows: the same neural device has the potential to be used for positive (e.g. assisting cognitive function in neurological patients) as well as negative purposes (e.g. identity theft and other forms of brain-hacking). It is worth noting that the attributes "positive" and "negative" with regard to technology use are hardly definable in an objective and non-contextual way. While the disambiguation of these terms remains an open philosophical question, a minimal characterization of *positive* in terms of "intended by design" and *negative* in terms of "unintended by design" may be helpful to roughly address the issue. Unlike dual-use dilemmas in personal computer technology, the dual-use dilemma of neural engineering is more radical as the object of dual-use (especially in the case of brain-hacking) is neural computation. Neural computation underlies life-maintaining processes (such as nutrition and respiration) as well as faculties such as consciousness, perception, thinking, memory and language and is primarily responsible for our behavior and our self-identification as persons – all the things that make us human. Therefore, misusing neural devices for cybercriminal purposes may not only threaten the physical security of the users but also compromise fundamental faculties of human beings, influence their behavior and alter their self-identification as persons. This dilemma is primarily faced not only by researchers and technology developers, but also by governments as they are committed to promoting health and security of their citizens.

Neuroprivacy, Neuroconfidentiality and Information Security

The possibility of extracting private and sensitive information from the brain of users represents a significant threat to privacy and data protection. Users that are victims of brain-hacking may lose the ability to seclude confidential or inherently sensitive information about themselves. For example, hackers could extract information about the character traits or sexual preferences of users. This sensitive type of information is potentially of interest not only to criminals involved in harmful activities such as blackmail but also to employers and insurances. For example, health insurance companies may be interested in extracting information about the medical records of the user to accept or reject her enrollment into an insurance plan or to determine her insurance premiums. This ethical problem is particularly significant because privacy is a priority issue in a free society, closely linked to civil liberties, democracy and human rights [4]. A famous adagio in information and computer security states: "the best antivirus software is your brain". This is meant to stress that the conscious choices made by the user are the most important determinants of the security of the user's computer system. The possibility of brain-hacking questions the adagio since it removes precisely this intermediate level of protection between the information and the hacker. In brain-hacking there is no external brain exerting control over the information in the computer through rational choices since that brain consists of exactly the same type of information under potential attack: neural information.

Autonomy and Personal Identity

The possibility for an external control over the user's future behavior poses a substantial threat to the moral principles of individual autonomy and agency and may even interfere with the self-determination of personal identity or personhood. Individual autonomy is generally understood as the capacity of someone to deliberate or act on the basis of one's self-chosen plan and not as the product of manipulative or distorting external forces [5]. By contrast, potential victims of brain-hacking may see their deliberation and action being constrained, controlled or manipulated by malevolent others. This problem is critical from an ethical perspective as the respect for autonomy is often considered the paramount principle of biomedical ethics. In fact, any notion of moral decision-making assumes that rational agents are involved in making informed and voluntary decisions. Autonomy also plays a key role in several legislations as a prerequisite for liability. For example, the USA Model Penal Code (MPC), Section 2.01, states that a person is not guilty of an offense when his liability is based on an involuntary act such as “a bodily movement that otherwise is not a product of the effort or determination of the actor, either conscious or habitual”. Users that are victims of brain-hacking would precisely fit in this description.

Conclusion

A Matrix-like future where people can access and manipulate information from other people’s brain is approaching rapidly. As neural engineering technologies become more and more widespread there is a fiduciary responsibility of experts to educate the population about what is reasonable to do. Collaborative research at the intersection between neuroscience, cybersecurity, bioengineering, criminal law and neuroethics is urgently required to assess these challenges and protect present and future users of neural devices.

Correspondence
Marcello Ienca, MSc, MA
Institut für Bio- und Medizinethik
Universität Basel
Bernoullistrasse 28
CH-4056 Basel

E-mail: marcello.ienca[at]unibas.ch

References

1. Rosenfeld JP. P300 in detecting concealed information. In Verschuere B, Ben Shakhar G and Meijer E (eds). Memory Detection: Theory and Application of the Concealed Information Test. Cambridge: Cambridge University Press; 2011, 63–89.
2. Martinovic I, Davies, D, Frank, M, Perito D, Ros T, Song D. On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. Paper presented at the USENIX Security Symposium, Bellevue, WA; 10–12 August 2012.
3. Conner M. (2010). Hacking the brain: Brain-to-computer interface hardware moves from the realm of research. EDN Network. 2010, 55(22);30–35.
4. American Bar Association (Privacy & Computer Crime Committee. Section of Science & Technology Law). International Guide to Privacy. Chicago, IL: American Bar Association; 2004.
5. Gillon R. Ethics needs principles – four can encompass the rest – and respect for autonomy should be “first among equals”. Journal of Medical Ethics. 2003,29(5):307–312.