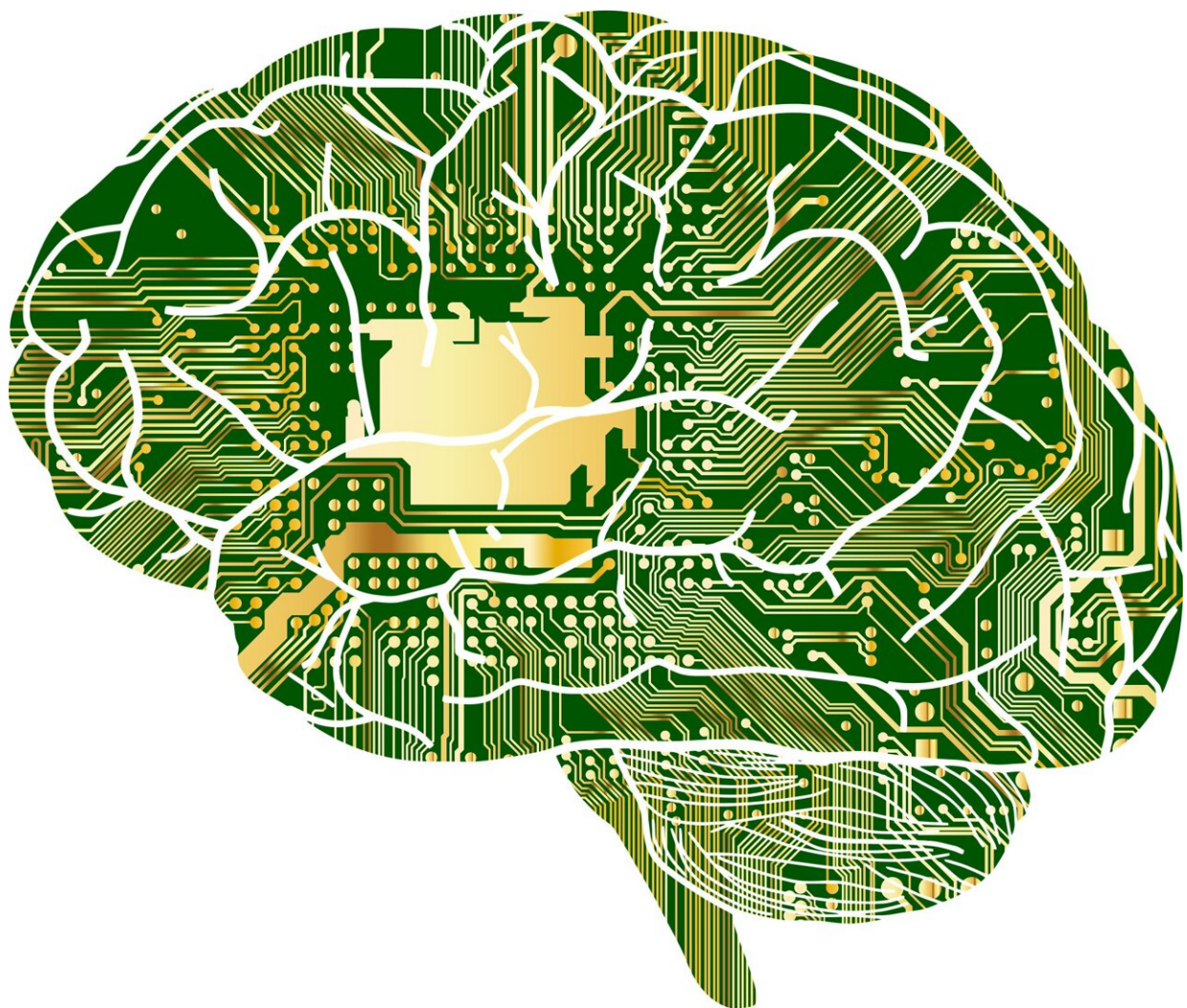


Neurodata can reveal our most private selves. As brain implants become common, how will privacy be protected?

February 14 2023, by Christina Maher



Credit: Pixabay/CC0 Public Domain

"Hello world!"

On December 2021, these were the [first words tweeted](#) by a paralyzed man using only his thoughts and a [brain-computer interface](#) (BCI) implanted by the company Synchron.

For millions living with paralysis, epilepsy and neuromuscular conditions, BCIs offer restored movement and, more recently, thought-to-text capabilities.

So far, few invasive (implanted) versions of the technology have been [commercialized](#). But a number of companies are determined to change this.

Synchron is joined by Elon Musk's Neuralink, which has documented a monkey playing the computer game Pong using its BCI—as well as the newer [Precision Neuroscience](#), which [recently raised](#) US\$41 million towards building a reversible implant thinner than a [human hair](#).

Eventually, BCIs will allow people to carry out a range of tasks using their thoughts. But is this terrific, or terrifying?

How do BCIs work?

BCIs can be non-invasive (wearable) or invasive (implanted). Electrical activity is the most commonly captured "neurodata," with invasive BCIs providing better [signal quality](#) than non-invasive ones.

The functionality of most BCIs can be summarized as passive, active and reactive. All BCIs use [signal processing](#) to filter brain signals. After processing, active and reactive BCIs can return outputs in response to a user's voluntary brain activity.

Signals from specific brain regions are considered a combination of many tiny signals from multiple regions. So BCIs use [pattern recognition algorithms](#) to decipher a signal's potential origins and link it to an intentional event, such as a task or thought.

One of the [first implanted BCIs](#) treated drug-resistant seizures in some of the 50 million people with epilepsy. And ongoing clinical trials [signal](#) a new era for neurologically and physically impaired people.

Outside the clinical realm, however, neurodata exist in a largely unregulated space.

An unknown middleman

In human interaction, thoughts are interpreted by the person experiencing and communicating them, and separately by the person receiving the communication. In this sense, allowing algorithms to interpret our thoughts could be likened to another entity "speaking" for us.

This could raise issues in a future where thought-to-text is widespread. For example, a BCI may generate the output "I'm good," when the user intended it to be "I'm great." These are similar, but they aren't the same. It's easy enough for an able-bodied person to physically correct the mistake—but for people who can only communicate through BCIs, there's a risk of being misinterpreted.

Moreover, implanted BCIs can provide rich access to all [brain signals](#); there is no option to pick and choose which signals are shared.

Brain data are arguably our most [private data](#) because of what can be inferred regarding our identity and [mental state](#). Yet private BCI companies [may not need to inform users](#) about what data are used to

train algorithms, or how the data are linked to interpretations that lead to outputs.

In Australia, strict [data storage rules](#) require that all BCI-related patient data are stored on secure servers in a de-identified form, which helps protect patient privacy. But requirements outside of a research context are unclear.

What's at risk if neurodata aren't protected?

BCIs are unlikely to launch us into a dystopian world—in part due to current computational constraints. After all, there's a leap between a BCI sending a short text and interpreting one's entire stream of consciousness.

That said, making this leap largely comes down to how well we can train algorithms, which requires more data and computing power. The rise of [quantum computing](#)—whenever that may be—could provide these additional computational resources.

Cathy O'Neil's 2016 book, [Weapons of Math Destruction](#), highlights how algorithms that measure complex concepts such as human qualities could let predatory entities make important decisions for the most vulnerable people.

Here are some hypothetical worst-case scenarios.

1. Third-party companies might buy neurodata from BCI companies and use it to make decisions, such as whether someone is granted a loan or access to health care.
2. Courts might be allowed to [order neuromonitoring](#) of individuals with the potential to commit crimes, based on their previous history or socio-demographic environment.

3. BCIs specialized for "neuroenhancement" could be made a condition of employment, such as in the military. This would blur the boundaries between human reasoning and algorithmic influence.
4. As with all industries where data privacy is critical, there is a genuine risk of neurodata hacking, where cybercriminals access and exploit [brain data](#).

Then there are subtler examples, including the potential for bias. In the future, bias may be introduced into BCI technologies in a number of ways, including through:

- the selection of homogeneous training data
- a lack of diversity among clinical trial participants (especially in control groups)
- a lack of diversity in the teams that design the algorithms and software.

If BCIs are to cater to diverse users, then diversity will need to be factored into every stage of development.

How can we protect neurodata?

The vision for "[neurorights](#)" is an evolving space. The ethical challenges lie in the balance between choosing what is best for individuals and what is best for society at large.

For instance, should individuals in the military be equipped with neuroenhancing devices so they can better serve their country and protect themselves on the front lines, or would that compromise their individual identity and privacy? And which legislation should capture neurorights: data protection law, health law, consumer law, or criminal law?

In a world first, [Chile](#) passed a neurorights law in 2021 to protect mental privacy, by explicitly classifying mental data and brain activity as a human right to be legally protected. Though a step in the right direction, it remains unclear how such a law would be enforced.

One US-based patient group is taking matters into its own hands. The [BCI Pioneers](#) is an advocate group ensuring the conversation around neuroethics is patient-led.

Other efforts include the [Neurorights Foundation](#), and the proposal of a "[technocratic oath](#)" modeled on the Hippocratic oath taken by medical doctors. An International Organization for Standardization [committee](#) for BCI standards is also under way.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: Neurodata can reveal our most private selves. As brain implants become common, how will privacy be protected? (2023, February 14) retrieved 27 April 2024 from <https://techxplore.com/news/2023-02-neurodata-reveal-private-brain-implants.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.