Promoting the Responsible Advancement of Neurotechnology

IBM has partnered with the Future of Privacy Forum to develop a whitepaper titled "Privacy and the Connected Mind: Understanding the Data Flows and Privacy Risks of Brain-Computer Interfaces" to explore this topic in depth. Excerpts from this whitepaper are included below.

Technologies that make interacting with computers more intuitive and seamless can offer huge benefits and transformative potential. Transitioning from punchcards to graphical user interfaces made using computers dramatically easier, and the subsequent development of laptops, smartphones, touch screens, and voice recognition brought about similar leaps in usability. As transformative as these new technologies were, their impact on how humans engage with technology will likely pale in comparison to the adoption of brain computer interfaces (BCIs) – devices that record, process, or analyze, or modify brain activity, invasively or non-invasively. Indeed, BCIs may be the last kind of user interface humans develop for computers – it's hard to get more seamless than connecting a computer to the human brain.

BCIs, and neurotechnologies more generally, are still emerging, but already offer impressive benefits in areas like healthcare where they are being used to diagnose medical conditions, facilitate rehabilitation, and control prosthetics. As neurotechnology and the use of neurodata matures, their exciting potential comes with difficult questions about how to address the potentially significant challenges they pose to privacy and consumer welfare. Policymakers, researchers, and other stakeholders should seek to proactively understand the risks posed by neurotechnology and develop technological and policy safeguards that precisely target these risks.

Key Terminology and Definitions

Neurodata: Data generated by the nervous system, which consists of the electrical activities between neurons or proxies of this activity.

Personal Neurodata: Neurodata that is reasonably linkable to an individual.

Neurotech/Neurotechnology: Technology that collects, interprets, infers, or modifies neurodata.

Brain-Computer Interface (BCI): Computer-based systems that directly record, process, or analyze brain-specific neurodata and translate these data into outputs that can be used as visualizations or aggregates for interpretation and reporting purposes and/or as commands to control external interfaces, influence behaviors, or modulate neural activity.

Some BCI implementations raise few, if any, privacy issues. For example, individuals using BCIs to control computer cursors might not reveal any more personal information than typical mouse users, provided BCI systems promptly discard cursor data. However, some uses of BCI technologies raise important questions about how laws, policies, and technical controls can safeguard inferences about individuals' brain functions, intentions, moods, or identity. These questions are increasingly urgent in light of the many potential applications of BCIs in:

***Healthcare* –** where BCIs could monitor fatigue, diagnose medical conditions, stimulate or modulate brain activity, and control prosthetics and external devices.

***Gaming* –** where BCIs could augment existing gaming platforms and offer players new ways to play using devices that record and interpret their neural signals.

***Education* –** where BCIs could track student attention, identify students' unique needs, and alert teachers and parents of student progress.

***Military* –** where governments are researching the potential of BCIs to help rehabilitate soldiers' injuries and enhance communication.

***Neuromarketing* –** where marketers could incorporate the use of BCIs to intuit consumers' moods and to gauge product and service interest.

***Smart Cities* –** where BCIs could provide new avenues of communication for construction teams and safety workers and enable potential new methods for connected vehicle control.

***Employment and Industry* –** where BCIs could monitor workers' engagement to improve safety during high-risk tasks, alert workers or supervisors to dangerous situations, modulate workers' brain activity to improve performance, and provide tools to more efficiently complete tasks.

While the potential uses of BCIs are numerous, BCIs cannot at present or in the near future "read a person's complete thoughts," serve as an accurate lie detector, or pump information directly into the brain. It is important for stakeholders in this space to delineate between the current and likely future uses and far-off notions depicted in science fiction so that we can identify urgent concerns and prioritize meaningful technological and policy initiatives. Many solutions to the challenges posed by neurotechnologies are technical in nature. To promote privacy and responsible use of BCIs, stakeholders should adopt technical guardrails, including:

- **Providing on/off controls when possible—including hardware switches, if practical;**
- **Providing users with granular controls on devices and in companion apps for managing the collection, use, and sharing of personal neurodata;**
- **Providing heightened transparency and control for BCIs that specifically send signals to the brain, rather than merely receive neurodata;**
- **Designing, documenting, and disclosing clear and accurate descriptions regarding BCI-derived inferences;**
- **Operationalizing industry or research-based best practices for security and privacy when storing, sharing, and processing neurodata;**
- **Employing appropriate privacy enhancing technologies;**
- **Encrypting personal neurodata in transit and at rest; and**
- **Embracing appropriate protective and defensive security measures to combat bad actors.**

However, policymakers and other stakeholders should also pursue policy and other governance mechanisms to minimize the risks posed by neurotechnologies and maximize their potential benefits. This includes:

- **Ensuring that BCI-derived inferences are not allowed for uses to influence decisions about individuals that have legal effects, livelihood effects, or similar significant impacts—e.g. assessing the truthfulness of statements in legal proceedings, inferring thoughts, emotions or psychological state, or personality attributes as part of hiring or school admissions decisions, or assessing individuals' eligibility for legal benefits;**
- **Employing sufficient transparency, notice, terms of use, and consent frameworks to empower users with a baseline of BCI literacy around the collection, use, sharing, and retention of their neurodata;**
- **Engaging institutional review boards (IRB) and other independent review mechanisms to identify and mitigate risks;**
- **Facilitating participatory and inclusive community input prior to and during BCI system design, development, and rollout;**
- **Creating dynamic technical, policy, and employee training standards to account for the gaps in current regulation;**
- **Promoting an open and inclusive research ecosystem by encouraging the adoption, where possible, of open standards for neurodata and the sharing of research data under open licenses and with appropriate safeguards in place. A similar open-skills approach could also be considered for a subset of direct-to-consumer BCIs; and**
- **Evaluating the adequacy of existing policy frameworks for governing the unique risks of neurotechnologies and identifying potential gaps prior to new regulation.**

As BCIs evolve and become commercially available, it is critical that policymakers understand both the risks these technologies pose as well as how these technologies work and what data is necessary for them to function. Because the neurotechnology space is still nascent, developers, researchers, and policymakers will have to strategically differentiate between real and hypothetical risks to develop meaningful solutions to promote privacy.

In the near future, BCI providers, neuroscience and neuroethics experts, policymakers, and societal stakeholders will need to consider what constitutes high-risk use in the field and make informed decisions around whether certain BCI applications should be prohibited – a position around which more robust and critical discussion is needed. Finally, and perhaps more fundamentally, it is also possible that the future of privacy itself and our notions of what it means to have or obtain privacy at basic human or societal levels could shift in ways that we cannot yet imagine.

Given all of this, it is therefore imperative that privacy professionals and other interested parties stay abreast of ongoing developments in this quickly growing space in order to innovate and regulate responsibly.