THE SciTech LAWYER

Neural Devices Will Change Humankind

What legal issues Will Follow?

An Examination of Security and Privacy Issues in Brain Computer Interface

By Stephen Wu and Marc Goodman

Published by the American Bar Association in The SciTech Lawyer, Volume 8, Number 3, Winter 2012.

NEURAL DEVICES WILL CHANGE HUMANKIND

What Legal Issues Will Follow?

By Stephen S. Wu and Marc Goodman

Though it is not widely known, brain implants and other neural devices have been successfully used for several years to treat neurological disease and brain injuries. In the future, these devices hold the promise of enhancing our quality of life and ultimately expanding the functionality of our minds. For instance, neuroprosthetic devices will interface with the nervous system to control prosthetic limbs. Moreover, new brain-computer interfaces and devices may someday duplicate some or all of the functionality of the human brain.

Some futurists and artificial intelligence experts envision credible scenarios in which synthetic brains will, within this century, extend the functionality of our own brains to the point where they will rival and then surpass the power of an organic human brain. At the same time, humans seem to have no limitations when it comes to finding ways to attack the computerized devices that others have invented. Attackers have successfully compromised computers, mobile phones, ATMs, telephone networks, and even networked power grids. If neural devices fulfill the promise of treatment, and enhance our quality of lives and functionality—which appears likely, given the preliminary clinical success demonstrated from neuroprosthetics—their use and adoption will likely grow in the future. When this happens, inevitably, a wide variety of legal, security, and public policy concerns will follow.

We will begin this article with an overview of brain implants and neural devices and their likely uses in the future. We will then discuss the legal issues that will arise from the intersection among neural devices, information security, cybercrime, and the law. Finally, we will close with our thoughts on how lawyers will deal with these new legal issues.

Stephen S. Wu, a partner in the Silicon Valley law firm Cooke Kobrick & Wu LLP, practices in the areas of information technology and intellectual property litigation and transactions, and served as the 2010–2011 Chair of the ABA Section of Science & Technology Law. Marc Goodman is the founder of the Future Crimes Institute and has worked globally with Interpol, NATO, and the United Nations on emerging technosecurity threats. He serves as Chair for Policy, Law & Ethics at Singularity University and participates in several committees of the ABA Section of Science & Technology Law.

The Development of Neural Devices

Brain-computer interface (BCI) or brain-machine interface (BMI) devices have been under development for a long time, with some devices having already reached the market. Currently, neural devices range from toys and games to research projects and some commercialized products. Turning first to toys and games, some companies are beginning to use brain wave technology. For instance, at the Game Developer's Conference in 2008, a company called NeuroSky, Inc. demonstrated a game in which users can manipulate objects on the screen with their thoughts alone. Both NeuroSky's MindWave and Emotiv's EPOC use sensors in an external headset to "read" the magnitude of users' brain waves and perform an action on the screen, such as moving a cursor or typing a key on a keyboard.[1] Similarly, a Star Wars-licensed product, The Force Trainer, is a toy in which a headset measures a child's brain waves and, when the child concentrates, converts brain waves into a signal to cause a ball to rise in a tube. Videos demonstrating these products are available on YouTube.[2]

Numerous research projects are underway to develop BCI technologies and neuroprosthetic devices. For instance, researchers are looking at the cellular level to determine how brain cells can control information technology processes. Researchers are also working on devices to control prosthetic limbs. One researcher cultured brain cells and used them to control a fighter plane flight simulator.[3] Other research projects in the neuroprosthetic area involve an interface between the nervous system and a device allowing a user to control a prosthetic limb. Next-generation devices may provide users with a "touch" sensation by using sensors in the prosthetic limb to transmit signals back to the brain.[4] Other research projects use "deep brain stimulators" to stimulate the brain, producing promising results for the treatment of Parkinson's disease, Alzheimer's disease, chronic pain, and other conditions.

Another fascinating research project concerns the study of how implantable medical devices directly attached to our brains can allow us to control a cursor on a computer screen, type, and send emails with our thoughts alone. This research involved attaching an interface device to a man who is paralyzed and unable to use his limbs to control a mouse or a keyboard. Such devices hold great promise to aid those with spinal injuries or diseases like Lou Gehrig's disease that impair movement.[5]

Perhaps the most common implanted neural device on the market now is the cochlear implant. Cochlear implants help the deaf or hearing impaired to hear better by taking in sound, converting it into electric signals, and interfacing with the nervous system so that the brain can receive and process the signals to generate sound in the mind of the wearer.

The Future of Neural Devices

In upcoming decades, we will continue to develop, sell, and use neural devices as toys and games, therapies for disease and injury, and for the purposes of further research. Some of the products that are in development will hit the market in upcoming years. Nonetheless, over the next half century, neural devices have the potential of radically enhancing the brain's functionality and ultimately

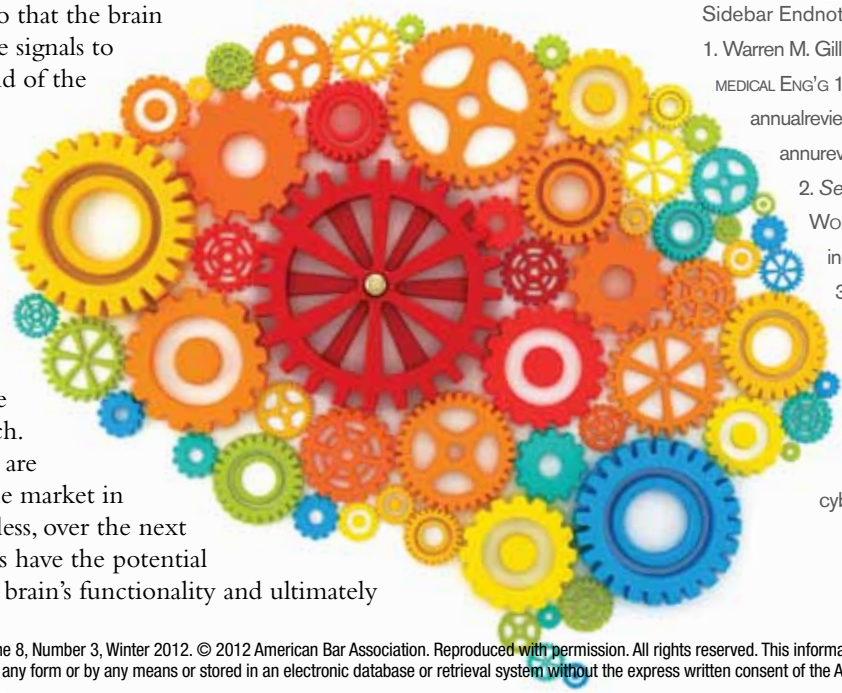

photo: istock photo

WHAT ARE NEURAL DEVICES?

"Neural interfaces are connections that enable a two-way exchange of information with the nervous system. These connections can occur at multiple levels, including with peripheral nerves, with the spinal cord, or with the brain. . . ."[1] Brain implants are a specific kind of neural device placed on the surface or the cortex of the brain that create an interface between the nervous system and microchips in order to treat damaged parts of the brain[2] or, in the future, to enhance its functionality. "By connecting intimately with computers, we will take the human brain to a new level. . . . If we can provide the brain with speedy access to unlimited memory, unlimited calculation ability, and instant wireless communication ability, we will produce a human with unsurpassable intelligence."[3]

Sidebar Endnotes

1. Warren M. Gill, et al., 11 Ann. Rev. Biomedical Eng'g 1 (2009), *available at* www.annualreviews.org/doi/pdf/10.1146/annurev-bioeng-061008-124927.
2. *See Brain Implant*, Article World, www.articleworld.org/index.php/Brain_implant.
3. Sherry Baker, *The Rise of the Cyborgs*, Discover Mag., Oct. 2008, *available at* http://discovermagazine.com/2008/oct/26-rise-of-the-cyborgs.

changing the human condition.

Some futurists predict that brain implants and other neural devices will dramatically expand the capabilities of the human brain. Chief among these futurists is Ray Kurzweil, who has written numerous books on the future of technology, including *The Singularity Is Near*.[6] These futurists point to trends such as exponential increases in speed and power of computer processors, the chief example of which is Moore's Law. Moore's Law holds that the number of transistors that can fit on a chip roughly doubles every two years. Moore's Law correlates with the speed and power of chips. With the benefit of ever more powerful computers and the miniaturization of computing devices, brain implants and other neural devices have the potential of showing similar exponential increases in speed and power. Futurists believe that such speed and power will give neural devices the capability of greatly enhancing the functioning of the human brain.

Even the benefits of enhanced memory through the use of information technology itself would radically change our lives. Right now, our organic brain has limited memory; we can only perceive and retain so much information at once, and we forget a great deal of information over our lifetimes. If we had devices directly connected to our brains that could enhance our memories, whether onboard in a brain implant or offboard in devices connected to our brains, we could learn new subjects rapidly and could recall and use information quickly. With the ever-increasing storage capacity afforded by information technology, we would not need to forget information—unless we wanted to. These technologies may significantly assist efforts to overcome diseases that cause the loss of memory.

Kurzweil and other futurists, however, go further than simply envisioning the use of information technology to enhance human brains. They believe that in this century, researchers will achieve ever-greater understanding of how the brain works. Coupled with exponentially advancing technologies, an enhanced knowledge of brain function will allow us to develop brain implants that have the speed, power, and memory to replicate the functionality of the entire human brain. Moreover, there is no reason why the brain must be limited to onboard devices. If we can connect devices to offboard devices, we will have potentially unlimited processing power and memory. In addition, the next logical step is to connect our neural devices to the Internet so that we can share, add to, and manipulate the entire world's information.

Kurzweil has predicted that around midcentury, computers and artificial intelligence will be so powerful, humans will be able to transfer ("upload") their lifetime's worth of memories to computers and carry on their thought processes and remember information using computers so that their thinking can be independent from their organic brains. Indeed, under this scenario, humans' thoughts and minds could outlive the death of the organic brain and physical body so that these humans would be functionally immortal. Their minds and thoughts would live on as processes run in computers. Hence, a *Time* magazine article describing this scenario bore the title "2045: The Year Man Becomes Immortal."[7]

Under Kurzweil's view, while ever more powerful information technology enhances the power of human brains, artificial intelligence (AI) will also become more powerful. Exponential technology advances will permit AI to rival and then surpass human intelligence. Because brain enhancement technology and AI will use many of the same methods, the distinction between the machine-enhanced organic human beings and AIs will blur. Consequently, Kurzweil predicts that by the end of this century, humans and robots using strong AI will be functionally indistinguishable.

The Information Security, Privacy, and Cybercrime Threats

Against this backdrop of sweeping changes in technology, we now examine the threats to neural devices from an information security and privacy perspective. Given the significant developments unfolding in the world of BCI and neuroprosthetics, we anticipate a wide variety of potential criminal threats to the human brain itself. First, people will have the means to attack neural devices. The media have publicized stories about hacking pacemakers and other medical devices. Attackers could use similar means to attack devices on board the human body, including wireless devices, controllers for prosthetic limbs, or deep brain stimulators.[8]

Second, people have the means and the motivation to exploit neural devices. Human ingenuity has no limitation, and unfortunately, the world has many people with the desire to use whatever weapons are at their disposal to defraud, terrorize, or otherwise harm other people. At a minimum, people already use technology to stalk, annoy, and steal from one another.

Third, the track record of the use of computers and the Internet shows that people will attack and subvert computers and devices if given the opportunity to do so. We have seen computer viruses, phishing, network intrusions, online fraud, unauthorized access, records snooping, trade secret theft, cyberbullying, cyberstalking, and numerous other forms of hacking and attacks. The history of computing and the Internet are replete with examples of ingenious people coming up with novel ways to harm other people.

In short, bad actors of various kinds, with various motivations, will inevitably attack neural devices, just as they have tried to attack computers, Internet-attached devices, and other medical devices.

The threat to neural devices, however, is different in kind from the threat to computers and the Internet. Early viruses caused annoyance as some hacker bragged about proving to the world he could inject malware into some piece of software by causing the screen to display a message saying, in essence, "Gotcha!" More malicious software caused more harm, such as erasing files. As malware became more sophisticated, attackers used it to steal money, technology, trade secrets, or national secrets. Other attackers sought to use denial of service attacks to bring down critical systems.

All of these conventional attacks affected, at least in the first instance, only money, data, and other property. It is true that such attacks could indirectly lead to injury or the loss of life, such as attacks on hospitals' computer networks, the theft of military technology, or the compromise of national security information. Nonetheless, none of the systems involved directly touched human beings, and so their compromise did not result in the immediate physical harm to a human.

The hacking of medical devices poses a different kind of threat. Medical devices maintain health and sustain life. Hacking such a device could result in immediate death or injury to a human. For instance, if an attacker turned off a pacemaker remotely, he could cause the user's heart to stop and immediately kill the user.

The use of neural devices entails an even greater risk than other medical devices. Attacking a neural device used to enhance a human's memory may have the effect of wiping out some or most of someone's memory or thought processes. Imagine a hacking attack that results in the equivalent of a lobotomy. A successful attack may not only harm the person physically or mentally, but it also may deprive the victim of the very essence of that person's humanity, his or her mind and memory. Disabling a prosthetic limb is one thing, but an electronic lobotomy is something quite different. Existing law criminalizing the conduct of a person that merely "intentionally accesses a protected computer without authorization"[9] does not begin to encompass or address the full significance of such a crime.

The Legal Issues of Brain Implants and Neuroprosthetics

Extrapolating from today's legal issues to the potential applications of neural devices in the future, we anticipate significant challenges to the legal system, including the following items.

Information Security and Privacy Policies and Controls

Companies that sell and provide services to support neural devices may have unique access to private information stored in the human brain—a depth and level of access that makes both Facebook and Google's archives seem feeble by comparison. Even the process of obtaining meaningful informed consent to the collection of data from an individual poses significant challenges. Device manufacturers will need to have data security policies to establish administrative, physical, and technical controls over the manufacture of neural devices and over the services that support such devices. Likewise, they will need privacy policies to address information practices relating to sensitive information and systems.

Information Security and Privacy Compliance

Federal and state laws may someday impose security and privacy requirements on manufacturers of neural devices and the companies that service them. Litigation arising from privacy torts and the violation of security and privacy requirements in statutes and regulations may crop up. Lawyers handling these matters may be specialists in information security and privacy laws, information technology transactions lawyers, or, in the case of privacy and security suits, litigators.

- **Products liability law:** Users whose devices are hacked may bring products liability, negligence, warranty, unfair trade practice, and related claims against manufacturers of neural devices for failing to implement security controls to prevent the compromise of these devices. Litigation lawyers will handle these matters.
- **Medical device regulation:** Manufacturers, importers, and other companies in the field will need to comply with Food and Drug Administration regulations when seeking to make or import neural medical devices. Regulations and the regulatory practice may involve obtaining: premarket clearance or approval; resolving disputes with the FDA; ensuring quality of the devices; dealing with FDA inspections; handling product recalls; and overseeing advertisements to consumers. Lawyers with an FDA practice handling medical devices will likely take on these matters.
- **Criminal law:** Criminal lawyers will likely take on matters of both substantive law and criminal procedure. For instance:
  - **Substantive criminal law:** States will need to come to grips with the new neural device technologies and create statutes to strike at those attacking neural devices. For instance, the intentional wiping of someone's stored memories should be a recognized crime. Some of the existing cybercrime laws would need to be updated as well. For example, is an attack on a brain implant analogous to a physical assault on a victim, such as a punch to the face? Likewise, if an attacker wiped the memories and functionality of a person's brain device, leaving the victim in a vegetative state, with what crime would we charge the attacker?
  - **Criminal procedure:** The courts will need to apply existing criminal procedural protections to those using neural devices. For

AS NEURAL DEVICES BECOME COMMONPLACE, **PRACTITIONERS WILL NEED TO LEARN MORE ABOUT THE TECHNOLOGY.**

example, if I have a neural device that stores my "memories" in the form of images, videos, text, and other files in my brain, can I prevent disclosures of this electronically stored information (ESI) on the basis of my Fifth Amendment right against self-incrimination? What if my neural device is connected to offboard storage? Does the fact that a third party holds those same files mean that I have no right to resist disclosure of this ESI under the Fifth Amendment due to the happenstance that the storage is off board instead of on board in my brain?

How Neural Devices Will Change Lawyers' Practices

We believe that the development and commercialization of neural devices is one example of the convergence of information technology and life sciences. Practitioners have an opportunity to create and shape a new area of law at the intersection of information technology and neuroscience. As lawyers have changed their practices to accommodate computers, the Internet, and other advances in technology, they will change their practices to take neural devices into account.

First, as neural devices become commonplace, practitioners will need to learn more about the technology. This step is the foundation for all science and technology law practices. The ABA Section of Science & Technology Law's committees provide forums for scientists, lawyers, and businesspeople to come together, learn about each other's fields, and create educational publications for the industry and bar. The Behavioral and Neuroscience Law Committee and Information Security Committee of the Section will, I am sure, work together in the future on these issues. Lawyers can talk with technologists and business contacts in their client organizations and work with multidisciplinary groups within the client to share views about the technology and its legal implications. Lawyers can provide crucial guidance to their clients that develop neural devices to build security and privacy protections into the devices and associated services during the design process.

Second, lawyers should help legislators, regulators, and groups like the Uniform Law Commission shape policy in the area of neural devices. We will need the good judgment of lawyers to inform policymakers about how existing laws apply to neural devices, where the law has gaps, and how new laws could address those gaps. At the same time, lawyers play a role in ensuring that any new legislation or regulations will protect the freedoms and protections we cherish.

Finally, lawyers will need to recognize where representing clients concerning neural devices will simply involve applying old law and methods to this new technology, and where new methods will be necessary. For instance, the FDA may require thorough assessments of privacy and security of neural devices during the approval process, where in the past it may have been more concerned with safety and effectiveness to treat disease and illness. In turn, FDA practitioners will need to become even more familiar with information security and privacy issues than they already are to respond to any FDA privacy and security requirements.

Brain implants and other neural devices may dramatically change the treatment of disease and injuries to the brain and nervous system. Over the long run, they may change humankind and what humans are capable of doing. Ultimately, the law will need to keep pace and lawyers with it. We may be witnessing the birth of a new field of law (public policy and security threats) at the intersection of neuroscience and information technology. We will be excited to see where this new field takes us. The time to consider these issues is now, before the use of these technologies becomes widespread and significant social harm takes place. ◆

Endnotes

1. See http://emotiv.com/ and www.neurosky.com for further information.

2. For instance, see the video at www.youtube.com/watch?v=6SFaPw5Mw0Y.

3. *See* Thomas B. Demarse & Karl P. Dockendorf, *Adaptive Flight Control With Living Neuronal Networks on Microelectrode Arrays*, *available at* http://neural.bme.ufl.edu/page13/assets/NeuroFlght2.pdf.

4. *See* David Brown, *For 1st Woman with Bionic Arm, a New Life Is Within Reach*, Wash. Post, Sept. 14, 2006, *available at* www.washingtonpost.com/wp-dyn/content/article/2006/09/13/AR2006091302271.html.

5. Andrew Pollack, *Paralyzed Man Uses Thoughts to Move a Cursor*, N.Y. Times, July 13, 2006, *available at* www.nytimes.com/2006/07/13/science/13brain.html.

6. Ray Kurzweil, *The Singularity Is Near* (2006).

7. Lev Grossman, *2045: The Year Man Becomes Immortal*, Time, Feb. 10, 2011, *available at* www.time.com/time/magazine/article/0,9171,2048299,00.html.

8. *See* Tamara Denning et al., *Neurosecurity: Security and Privacy for Neural Devices*, J. of Neurosurgery (July 2009).

9. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(B).