The Internet of Bodies: Enhancement Technologies and Governance Challenges

Prof. Dr. Heba Gamal El-Din,
Head of the Department of Future Studies, National Institute of Planning

The Internet of Bodies (IoB) has emerged as a part of enhancement technologies designed to create bodies more capable of surviving and adapting to new changes, according to Darwin's theory of evolution. This is achieved by augmenting the human body with artificial intelligence technologies to break human limitations, expand human capacities, and overcome diseases, aging, and disabilities. Some proponents of transhumanism even entertain the notion of overcoming death, categorizing it as a disease that can be conquered to achieve immortality. Although this idea (overcoming death) may seem naive and unrealistic, it is a subject of research at major US and EU universities, such as Harvard University; this subject is also an area of interest for biotechnology companies like Stemcentrx and Breakout Labs.

To start with, enhancement technology has become one of the modern tools of life application; it embodies Darwin's concept of natural selection, which means adapting to the local environment for survival and reproduction. Through this process, humans gradually acquire beneficial and healthy traits passed down from generation to generation. However, does every evolution solely include beneficial and healthy traits? Moreover, are there inherent challenges that require careful consideration and study on how to ensure good governance of these modern technologies while respecting the ethics of science, religion and national security requirements?

In essence, the Internet of Bodies (IoB) integrates machine technology with humans through a network of internet-connected devices and technologies that interact with the human body. This concept is an extension of the Internet of Things (IoT) but it focuses on the human body, targeting its health condition. IoB partly means that human bodies rely on the internet and related technologies, such as artificial intelligence, for their safety and functionality.

This technology emerged in 2016 and was considered a core part of the Internet of Things, through which users monitor their bodily movements, heart rates, and exertion levels, obtaining detailed health information. The term's origin is attributed to Professor Andrea M. Matwyshyn, an expert in law and engineering, who applied it to develop public policies and regulatory laws. The Internet of Bodies is defined as a collection of internet-connected smart devices that monitor the human body, gather health and other personal data, and transmit this data over the internet. These devices collect vast amounts of personal biometric data through physical measurements such as height, weight, hair color, and skull measurements, as well as individual behavioral data about a person's body functions and how they enhance cognitive abilities, memory, and record anything the user sees through a lens implanted in the eye or equipped with a camera.

An IoB device includes software or computational capabilities and communicates with an internet-connected device to gather generated health or biometric data, altering human body functions. Generally, IoB devices require physical contact with the body, worn, ingested, implanted, or otherwise attached to or embedded in the body, either permanently or temporarily. Some IoB devices are medical devices regulated by the Food and Drug Administration.

Generations of the Internet of Bodies

The Internet of Bodies (IoB) has evolved through several generations. The first generation includes external devices connected to the human body and the internet, such as earbuds, smart clothing, and fitness tracking devices like smartwatches, rings, and glasses that use sensors to monitor steps and heart rate. The second generation involves the implantation of artificial devices within the human body, such as pacemakers, blood pressure monitors, insulin pumps, and smart prosthetics integrated into patients' nerves and muscles, or even digital pills that transmit medical data after ingestion. The third generation comprises devices that fully integrate into the human body, maintaining immediate connectivity with external devices and the internet. A notable company in this field is Neuralink, an Elon Musk enterprise developing an implantable chip that connects the brain to a computer, capable of reading brain signals from a paralyzed person to help control an external device.

For instance, a pacemaker can provide continuous real-time information about a patient's heart fluctuations, regulate the heart rate in cases of extreme speed or slowness, and aid in treating heart failure, thereby improving the patient's quality of life and, in many cases, preserving it.

Digital or smart pills first emerged in 2017 when the U.S. Food and Drug Administration (FDA) approved the first digital pill with embedded sensors to record medication intake. These pills, used for treating schizophrenia, certain forms of bipolar disorder, and depression, are redesigned to include a sensor that sends messages to a mobile app to monitor medication adherence via smartphones. This allows doctors to legitimately intervene if patients miss their medication, preventing relapses. This development signifies that the human body has become legitimately and comfortably penetrable.

And how can healthcare provider networks be protected and secured from cyber attacks. Additionally, there is the potential for recurring risks that plague Internet of Things (IoT) devices with the Internet of Bodies, as the same security flaws found in IoT devices or any other technology that stores information in the cloud could be present. Security vulnerabilities can allow unauthorized parties to leak private information.

The implantation of chips in the human body, either directly or via vaccines and aluminum microchips accumulating in the body post-vaccination, is another example. In May 2022, the FDA granted Neuralink a license to begin human trials of their chip, despite previous refusals to ensure human physical safety. In 2024, Neuralink successfully implanted a brain chip in a human, with ongoing studies to enable people to control computers with their minds and assist those with cerebral palsy, visual, or auditory impairments to interact with society. Additionally, in the same year, doctors at the Max Planck Institute in Germany developed a chip-sized robot capable of performing precise operations in the human intestines without surgical intervention.

By 2021, we witnessed the existence of a human cyborg who transitioned from complete paralysis to mobility and interaction through internally implanted artificial devices controlling all vital functions, in the unique experiment of "Morgan Peter Scott."

With all these advancements, questions arise regarding the governance of such technologies and the ability of governments to regulate them, protecting citizens from the risk of body hacking, which has become legitimate through a series of scientific conferences since 2018, legalizing and regulating it (Legal Bio Hacking), or the emergence of health tracking technology. There is also concern about countries controlling others through imported drugs and vaccines.

Internet of Bodies Technology: Governance Challenges

This technology presents several risks, particularly concerning the governance challenges of protecting the human body from hacking and intrusion, which could threaten overall safety and life. One key issue is the equitable distribution within a country, where only the wealthy can afford these advanced technologies and enhance their bodies, leaving the poor behind. Additionally, there are disparities between developed and developing countries, where some nations produce the technology, and others consume it, leading to control by the producing countries. There are also religious concerns, as this technology alters human nature and may pose a threat to human safety. Moreover, issues of autonomy, decision-making, and the validity of decisions made by individuals enhanced with IoB technology arise. Establishing optimal standards for the security of implanted medical devices and protecting healthcare providers' networks from cyberattacks is also crucial.

The National Institute of Standards and Technology (NIST) collaborates with public and private sector partners to develop best practices for managing cyber risks. They work with the Medical Device Innovation Consortium to disclose medical device vulnerabilities without fear of civil liability or criminal prosecution

Egypt faces the challenge of studying these issues, addressing them, and empowering relevant authorities to govern IoB-based devices. This includes developing purchasing and import regulations for modern medical devices and encouraging private and civil sectors to collaborate with the government on policies related to security, health, and safety issues, and scrutinizing imported drugs and vaccines to ensure their safety. Encouraging scientific research is also essential as a starting point for technology localization in Egypt

IoB technology could replicate the risks associated with the Internet of Things (IoT), including the same security flaws. These vulnerabilities could allow unauthorized parties to leak private information, manipulate data, or deny users access to their accounts. In the case of some implanted medical devices, hackers could potentially manipulate the devices to cause physical harm or even death. There is also the possibility of controlling the decisions of states through non-state actors by manipulating the vital data and devices of leaders.

Addressing these issues is a significant focus for the U.S. Food and Drug Administration (FDA), legislative committees in Congress, medical research centers, and security agencies. This creates a challenge for the Egyptian Drug Authority and legislative and security bodies to scrutinize these issues and examine their legality.

Notable efforts in IoB governance include the "Hippocratic Oath for Connected Medical Devices" by the organization I am the Cavalry, which outlines five voluntary principles for healthcare providers and device manufacturers to adopt for better patient safety and security. These principles emphasize the importance of ensuring the resilience of devices and the data they contain against hacking, interception, manipulation, and unauthorized disclosure while ensuring their effectiveness and timely repair and improvement.

The National Institute of Standards and Technology (NIST) collaborates with public and private sector partners to develop best practices for managing cyber risks. They work with the Medical Device Innovation Consortium to disclose medical device vulnerabilities without fear of civil liability or criminal prosecution. The FDA collaborates with MITRE Corporation to develop a scoring system to rank the severity of software vulnerabilities in medical devices as a tool for tracking potential health and safety impacts on patients whose medical devices are hacked. These efforts aim to assess and prioritize risk points and vulnerabilities. However, issues of coercion and jurisdiction remain unresolved.

In response, some regions have enacted laws to protect citizens and their privacy, such as California's biometric data privacy law, which took effect in 2020. This law grants individuals the right to know what information is collected about them, the purposes of collection, and the entities with which this information is shared. It also allows individuals to opt out of having their personal data sold and requires businesses to delete records upon consumer request. However, this law is specific to California and needs further development to become a binding international law.

In conclusion, there remains the challenge of readiness, access, and enforcement in the absence of scientific ethics and defined practice boundaries. Egypt faces the challenge of studying these issues, addressing them, and empowering relevant authorities to govern IoB-based devices. This includes developing purchasing and import regulations for modern medical devices and encouraging private and civil sectors to collaborate with the government on policies related to security, health, and safety issues, and scrutinizing imported drugs and vaccines to ensure their safety. Encouraging scientific research is also essential as a starting point for technology localization in Egypt.