APRIL 2023

BODIES ONLINE, SOULS OFFLINE

THE INTIMATE INVASION: EXPLORING THE DANGERS OF THE INTERNET OF BODIES

TECH HIVE ADVISORY

ABOUT TECH HIVE™

Tech Hive Advisory Limited ("Tech Hive") is a technology policy advisory and research firm providing services to private and public organisations regarding the intersection between technology, business, and law. We focus on how emerging and disruptive technologies are altering and influencing traditional ways of doing things while acting as an innovation partner to our clients.

Our expertise and experience span Research and Policy Advisory, Privacy and Data Protection, Data Ethics, Cybersecurity, Regulatory Intelligence, Start-Up Advisory, Emerging Tech, and Digital Health. We ensure that our advice is useful to our clients by thoroughly understanding their businesses and the markets in which they operate, which we accomplish through accurate policy and legislative development tracking and intelligence.

Contact: contact@techhiveadvisory.org.ng

CONTRIBUTORS

Adedolapo Adegoroye
Diana Uzor
Dorcas Tsebee
Martha Apeh
Omowumi Adewumi
Precious Nwadike
Tersoo Ayede
Victoria Adaramola

EDITORS

Nurudeen Odeshina
Ridwan Oloyede

Disclaimer - Usage of Research
The research is intended to be general and educational in nature, rather than legal advice, and should not be construed as such. The information and materials from the study may not apply to all (or any) situations. As a result, they should not be implemented without the advice of qualified legal counsel.
The absence of a trademark or service mark from this list does not imply that Tech Hive has relinquished its intellectual property rights in relation to that name, mark, or logo.

EXECUTIVE SUMMARY

The Internet of Bodies (IoB), like the Internet of Things (IoT), is one of technology's astounding innovations, presenting a relationship between humans and devices (technology). IoB is a subset of the Internet of Things that connects the human body to a network via devices that are implanted, ingested, or connected to the human body to perform a specific function. The IoB enables a form of intimacy between humans and a variety of devices, including smart watches, smart pills, pacemakers, and fitness trackers, among others. These devices examine the human body, collect personal data, and transmit the information to the internet for a response.

IoB has indeed revolutionised every industry in which it has been adopted, most notably the healthcare sector, in which these devices are frequently used to monitor health functions and data. The research focused on what IoB means as a subset of IoTs, its many global use cases, its benefits, the regulatory framework in Nigeria, and the privacy and security risks associated with their applications.

Based on an analysis of the available data, the research found the following:

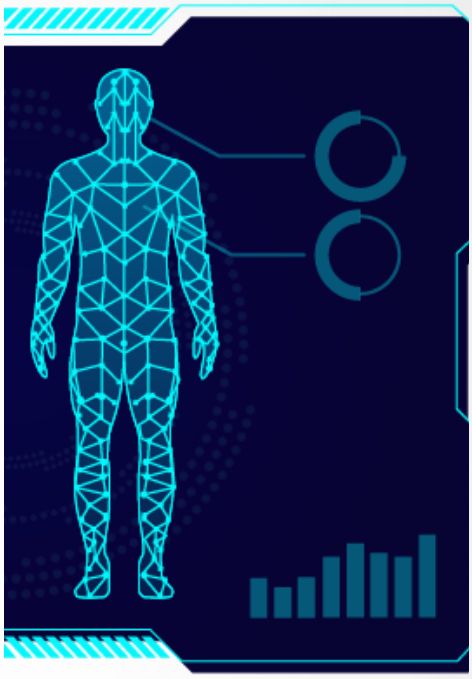
- IoB devices are capable of and have revolutionised the healthcare system in remarkable ways by making life easier for everyone;
- There is a lack of adequate and comprehensive legal framework for the regulation of IoB devices and its uses in Nigeria;
- When interacting with humans, IoB devices collect a vast amount of personal information, posing significant privacy risks for users; and
- Users of IoB devices face security risks due to the variety of data collected by these devices and the ambiguity surrounding their use.

Based on the findings of this research, the following recommendations have been made:

- Development of a comprehensive regulatory framework for IoB devices and their users;
- Adoption of specific data protection considerations and principles to combat unauthorised access to and misuse of personal data; and
- Adoption of security considerations in the development and utilisation of IoB devices.

INTRODUCTION

Technology continues to play a vital role in the search for permanent cures for terminal diseases and in efforts to improve healthcare. Over the past century, technological progress has revolutionised healthcare delivery. Breakthrough technologies like stem cells, gene therapy, biotechnology, regenerative medicine, immunotherapy, digital therapeutics, nanotherapy, telemedicine, and predictive medicine, among others, are having a significant impact on the healthcare industry. Importantly, new technologies like artificial intelligence, 3D printing, augmented and virtual reality, and the Internet of Things are making their way into mainstream healthcare delivery. [1]



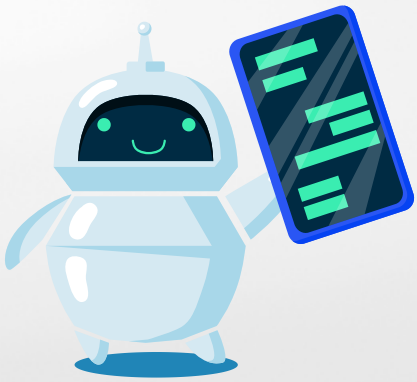
The Internet of Bodies (IoB) is a subset of technologies that fall under the "Internet of Things" (IoT) umbrella.[2] IoB are made to monitor, check, or interact with the human body in a certain way. IoB uses human bodies as a data source, making it a component of the Internet of Things ecosystem.[3] They are made up of human bodies or body parts that are linked to a network or a network array with the goal of generally improving or providing insights to improve the human body. IoBs create a much more intimate relationship between technology and the human body. They are networked devices that monitor the human body, collect physiological, biometric, or behavioural data, and exchange data over a wireless or hybrid network.[4]

The "Internet of Bodies" (IoB) has been continuously deployed to improve the quality of human life and existence in mind-bogglingly innovative ways.[5] However, they may be as intrusive to privacy as they are life-saving. [6]

When it comes to innovative technology, the desire to explore its potential and possibilities almost always outweighs privacy, security, and policy concerns. There are numerous advantages to these technologies that some believe are too significant to be stifled by a lack of policy.[7] The inherent benefits of technology should not be discounted out of fear of hype, but it is important to make the distinction between hype and reality.

Internet of Bodies are classified into three generations of devices: the external body, which is the first generation; the internal body, which is the second generation; and the embedded body, which is the third generation.[8] The first generation refers to a wider range of devices that are worn on or physically connected to a human body and collect and transmit data based on physical contact through sensors, computer vision, and so on. The second generation is more technical, as they are placed internally in the human body and may be ingested or surgically implanted to control and monitor various conditions of the human body. The third generation, which is currently the last classification and is not nearly as common.[9] They are embedded in the human body and have real-time access to a remote machine.[10]An example would be the much-elusive Brain-Computer Interface (BCI), where the human brain merges with an external device, allowing for a real-time connection with remote computers that receive live data updates for the purposes of controlling and monitoring.[11]

IoBs, like IoTs, offer numerous opportunities for human advancement; however, they also pose significant risks and vulnerabilities that could turn into nightmares for users. With IoT, there are growing concerns about constant surveillance over people and their surroundings, and with IoB, these concerns extend beyond environmental surveillance to include humans losing autonomy over their lives and human bodies.[12] Without appropriate policies, legal frameworks, and futuristic preventive laws, these innovative technologies have a tendency to create larger problems than they can attempt to solve.[13]



A SYMPHONY OF CONNECTIVITY: THE INTERNET OF BODIES AND AND ITS ENCHANTING USE CASES

IoB applications range from better diagnosis and treatment of medical conditions to personalised care, increased productivity, and improved public safety, to name a few. IoB has been of tremendous benefit to healthcare, revolutionising both preventive and diagnostic care.

IoB products and solutions are developed to solve a multifarious system of problems in the healthcare system. Most IoB products come in direct contact with the human body, are physically attached to it, or, as in the case of ingestible and implantable devices, are swallowed or surgically inserted into a patient's system.[14] There are many instances in which IoB improves healthcare. Wearable physical activity trackers like smartwatches that can monitor daily exercise, heart rates, blood pressure, and even sleep cycles provide the user with a vast amount of personal data about themselves that could improve preventive healthcare and inform them on when to take breaks or get more physically active.[15] They are capable of informing the users to become more active participants in paying attention to their health. Furthermore, wellness technology devices such as smart cribs and smart pads could notify and inform when there needs to be a change.

With the use of smart cribs, parents or guardians can get mobile notifications of the condition of their babies based on their body temperature, how active their baby is, and whether they are asleep or awake.[16]

Connected bras and breast cups, smart glucose metres, and wearable insulin pumps also keep users up to date on the state of their bodies and when and what changes should be made over time.[17] For example, a person with diabetes could easily monitor their blood sugar in real time to enable easier maintenance of healthier blood sugar levels as well as quick and immediate response to prevent health dangers.[18] Artificial organ systems, digital pills, and brain-computer interfaces with sensors could also be implanted to improve the functionality of the human body. Brain-computer interfaces could allow amputees to control prosthetic limbs with their minds.[19]

Furthermore, IoB can be incorporated into healthcare wearable devices or in the sports industry. They perform similar functions as they do in the healthcare industry. Wearable devices are used to monitor and improve the performance of athletes.[20] IoB can be used to monitor athletes and understand how they respond to specific exercises and activities. This helps to develop better exercise, and sporting strategies can be developed for athletes. Also, IoB can be used to detect injuries, including non-visible injuries, so that they can be treated on time.[21] This benefit also extends to people who engage in sports activities or exercises for recreational purposes or any other purpose.

Despite the benefits of IoB to the healthcare system, they are still quite sensitive because, as much as there are enormous benefits, we have to consider the rate and risk attached to the processing of sensitive personal data.

The contentious issue of whether data collected from an IoB device or product that was originally implanted or worn with the goal of improving the functions of the human body could be used as evidence in a court of law was raised in a well-known Michigan case.[22] Should life-saving or life-enabling devices be used as a tool for surveillance, monitoring, and control over a person's life?

In the popular case, a suspect's artificial heart implant, which was installed to support his heart functions was used as evidence against him on his charge for arson. To establish the case, the police got a warrant for all electronic data stored in the suspect's heart implant. Data collected from the heart implant was used to provide a report on his heart activity at the time of the crime incident, and the expert witness stated that it was highly unlikely for the suspect to have escaped the fire at his residence along with his valuables through the window as the suspect had claimed.[23]

IoB however, goes beyond just healthcare improvements and has been deployed in the military, sports, and event security.[24]IoB devices are used in the military to monitor a soldier's emotional and physical state, as well as to track vitals and location. It can also be used to simulate real-life combat situations, allowing soldiers to practise and perfect multiple combat strategies.[25]The use of IoB in the military makes it easier for militaries to locate wounded soldiers and provide medical aid to affected soldiers as needed. In sports, IoB can be incorporated into fabrics, helmets, wristbands, and other wearable devices used by athletes in the sports industry.[26]IoB can be used to monitor athletes and understand how they respond to specific exercises and activities. This helps to develop better exercise, and sporting strategies can be developed for athletes.

THE GIFT OF HARMONY: EMBRACING THE TRANSFORMATIVE BENEFITS OF THE INTERNET OF BODIES

The Internet of Things has made the world a better place. The advantages of IoB devices are numerous and can be seen in a variety of industries, most notably the healthcare sector.[27] Implementing IoB technologies in the healthcare system has resulted in improved health condition diagnosis and treatment, personalised insurance packages, and increased productivity.[28]

As previously stated, healthcare professionals are the immediate beneficiaries of the IoB revolution.[29] The benefits include the following:

a. **Patient monitoring**: IoB devices enable caregivers to detect changes in a patient's physiological data and take appropriate action in the event of an emergency. As an intermediary, the IoB reduces the risk of contracting diseases through physical contact. The significance of these sensors and camera-based IoT devices was notable during the covid-19 era, when doctors were required to maintain a safe distance from patients unless they were properly masked.[30]

b. **Improved healthcare delivery**: VivaLNK, a Silicon Valley technology company, has created a revolutionary smart thermometer that nurses are using to take the temperatures of Covid-19-diagnosed patients, thereby improving healthcare delivery.[31] A single sensor records the temperature of each individual patient, thereby minimising human contact and reducing the risk of virus transmission. The information is then transferred to a monitoring dashboard. If the results are abnormal, healthcare professionals are alerted and can then take the appropriate action.[32] As smart thermometers collect data over time, this enables medical professionals to identify and analyse long-term trends with the ultimate goal of enhancing patient care.[33]

c. **Non-invasive diagnosis**: Doctors in the United States use camera-based ingestible pills as an alternative to gastroscopy and colonoscopy, which may require physical contact with the patient's body.[34] Developed IoB devices that can be worn on the body of a patient to detect abnormalities in a patient's system aid in early detection of lung problems.[35] Furthermore, wearable sweat sensors have been developed to analyse body functions, and doctors can use this data to diagnose genetic disorders and better treat health conditions such as diabetes.

d. **Improved quality of life**: By removing and replacing affected body functions, IoB technologies have enhanced the quality of life of patients with chronic health conditions. There are devices such as connected pacemakers that transmit data to a detected mobile application, microelectronic retina prostheses that restore partial vision to individuals with retina diseases, and automated insulin delivery systems that monitor blood sugar levels in real time.[36]

e. **Precision medicine**: IoB devices also assist health professionals in analysing and identifying recurring patterns in health data, as well as developing personalised medication and treatment plans that are tailored to a patient's unique health conditions. With the patient's medical history, the physician is better equipped and in a better position to develop a treatment plan for the patient(s). Here, sensor data and AI will be used to analyse electronic health records.[37]

f. **Personalised health insurance plans**: On the basis of the personal data collected by IoB devices, health insurance companies can adopt a more customised insurance plan that takes into account the insured's medical

history, occupation, and lifestyle.[38]

g. **Increased productivity**: IoB devices, like other innovations over the years, increase human productivity by making things easier.[39] IoB researchers have reached a uniform conclusion on how much better the world has become since the introduction of IoB devices. This ranges from smart home devices to hearing aids and pill dispensers, just to mention a few.

h. Fitness technologies have been developed that track exercises and weight-measuring equipment enhanced with sensors. This helps with fitness goals and consistent fitness tracking.[40]

i. Wellness technologies such as baby tech solutions help with baby care by sending signals about babies, such as their temperature and when diapers need to be changed. There are also Femtech products such as smart pads, tampons and menstruation cups, connected bras and breast cups, hardware fertility trackers and so on that help with feminine body awareness and care.[41]

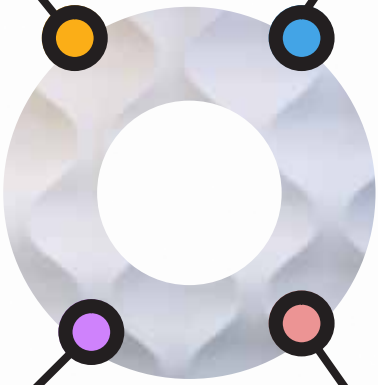
NAVIGATING UNCHARTED WATERS: THE EVOLVING LEGAL LANDSCAPE FOR THE INTERNET OF BODIES IN NIGERIA

GENERAL LAWS

- The Constitution of the Federal Republic of Nigeria 1999
- Freedom of Information (FOI) Act 2011
- Law Reform(Torts) Law, Ch. L82 Laws of Lagos State
- Evidence Act, 2011
- Standards Organisation of Nigeria Act of 2015
- National Agency for Food and Drug Administration and Control Act 2004
- Federal Competition and Consumer Protection Act

BILLS

- Nigerian Data Protection Bill 2022
- National Electronic Health Record Bill



HEALTH SECTOR LAWS

- National Health Act 2014
- National Health Insurance Scheme Act (NHIS Act) 2004
- The Lagos State Health Sector Reform Law
- The Medical and Dental Practitioners Act
- The Code of Medical Ethics in Nigeria (Rules of Professional Conduct for Medical & Dental Practitioners)
- Nigerian National e-Health Strategy 2011
- National Health Policy 2016
- FCT e-Health Policy and Policy Implementation Strategy
- Nigerian Health Information System Policy 2014
- FCT e-Health Policy and Policy Implementation Strategy
- Guidelines on Document and Record Retention

DATA PROTECTION AND CYBERSECURITY LAWS

- Nigeria Data Protection Regulation, 2019
- Cybercrimes (Prevention and Prohibition) Act
- Guidelines For the Management of Personal Data by Public Institutions in Nigeria, 2020
- Nigeria Cloud Computing Policy
- National Information Systems and Network Security Standards and Guidelines 2013
- Nigeria National Cybersecurity Framework
- National Cybersecurity Policy and Strategy 2021
- National Cybersecurity Policy/Strategy Implementation Guidelines for Ministries, Departments & Agencies (MDAs) & Private ICT Organisations

KEY SOURCES OF INTERNET OF BODIES LAW IN NIGERIA

THE CONSTITUTION

The Constitution provides for a right to life,[42] dignity[43] and privacy.[44] The right to privacy extends to the right to privacy of medical records and health information as well as the right to privacy in the digital economy. Any technology that enables IoB must have regard to these fundamental rights of the users.

EVIDENCE ACT

By virtue of the Evidence Act[45] computer-generated evidence is admissible in court. This includes all data transmitted through IoB technologies.

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY ACT

The National Information Technology Development Agency ("NITDA") administers the National Information Technology Development Agency Act. The agency coordinates the general information technology development in Nigeria. The Agency has issued several guidelines and policies to this effect. The Nigeria Data Protection Regulation 2019 was issued by the NITDA which is currently the primary legislation on data protection in Nigeria.

NIGERIA DATA PROTECTION REGULATION 2019

The Nigeria Data Protection Regulation ("NDPR") is the most comprehensive data protection legal framework in Nigeria. It creates different obligations for data controllers and processors, which include ensuring security, creating mechanisms

for protecting data subjects' rights, implementing the data protection principles, and building governance and accountability measures, among others. The principles and obligations have an impact on the use of IoB, from ensuring the safety of the equipment to responsible data processing, transparency around data processing, and operationalising the data subject rights mechanism, among other obligations. Healthcare facilities that use IoBs, as well as device manufacturers, will be required to follow the law's requirements.

GUIDELINES FOR THE MANAGEMENT OF PERSONAL DATA BY PUBLIC INSTITUTIONS IN NIGERIA

By virtue of these guidelines, federal and state-owned hospitals as well as other public institutions that use IoBs must adhere to the data protection standard introduced by the guidelines. The guidelines impose a higher standard of consent for the processing of sensitive data, such as health data. The consent to process sensitive data must be direct, unambiguous, and distinct.[46] This is similar to the position under the NDPR. The document is useful when the device is deployed in public health institutions.

MEDICAL AND DENTAL PRACTITIONERS ACT

The Medical and Dental Practitioners Act establishes the Medical and Dental Council of Nigeria ("MDCN")[47] to regulate the practice of medicine, dentistry, and alternative medicine in the most efficient manner that safeguards the best health care delivery for Nigerians. It also establishes a panel[48] and a tribunal[49] to entertain any complaint against a medical practitioner for misconduct.

The MDCN has also established a code of conduct[50] which medical practitioners must adhere to in the course of their profession. The code mandates medical practitioners to obtain consent for invasive and non-invasive medical procedures.[51] Before obtaining consent, medical practitioners must counsel patients on the expectations of the procedure in simple terms; a failure to do this may amount to assault on the patient. A medical practitioner is also bound by confidentiality obligations to the patient; they may not reveal health information to third parties.[52]

NATIONAL HEALTH ACT

The National Health Act provides a framework for the regulation, development, and management of a health system and sets standards for rendering health services in Nigeria. The Act provides that any person who intends to establish, construct, modify, or acquire health technology must obtain a certificate of compliance to do so.[53] Failure to obtain a certificate of standard is an offense punishable by a fine, imprisonment, or both.[54] In addition, it imposes obligations on healthcare providers to ensure privacy, confidentiality, and security in care delivery.[55]

CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT 2015

The Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 ("Cybercrimes Act") is a comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. The Act aims to create a system for the protection of computer systems and networks, electronic communication, intellectual property and privacy rights.[56]

The Act defines a computer system as any device or group of interconnected or related devices that performs automated or interactive processing of data.[57] By this definition, technological devices facilitating the IoBs are computer systems protected against unlawful access, modification, interception, among other interference.

NATIONAL AGENCY FOR FOOD AND DRUG ADMINISTRATION AND CONTROL ACT

The Act establishes the National Agency for Food and Drug Administration and Control ("NAFDAC") which is charged with the responsibility to regulate and control the importation, manufacture, and use of medical devices as well as make pronouncements on their quality and safety. Any instrument, apparatus, or contrivance (including components, parts, and accessories thereof) manufactured for internal or external use in the diagnosis, treatment, mitigation, or prevention of any disease, disorder, abnormal physical state, or the symptoms of a disease in a human are referred to as a medical device.[58]

STANDARDS ORGANIZATION OF NIGERIA ACT 2015

This Act establishes the Standards Organisation of Nigeria. The aim of the Act is to standardise methods and products in Nigerian industries. It performs quality monitoring and control for goods, including IoB devices produced and imported into Nigeria.

OTHER SOURCES OF LAW

LAW OF TORTS

The use of IoB devices is also likely to sometimes result in unprecedented events as a result of bodily injury. The existing regulatory gaps mean that some IoB products will potentially be subject to no preemptive regulatory scrutiny before entering the market.[59] The state of existing laws also makes it more likely that plaintiffs will turn to tort law to address the failures in these products that cause physical harm to human bodies.[60] Currently, most of the harm experienced by IoB consumers is related to privacy and security, which has posed a challenge for private litigants to demonstrate actual economic losses in the eyes of the courts. However, the economic loss will often be more easily quantifiable and economically demonstrable in IoB contexts than was possible in previous generations of software cases.[61]

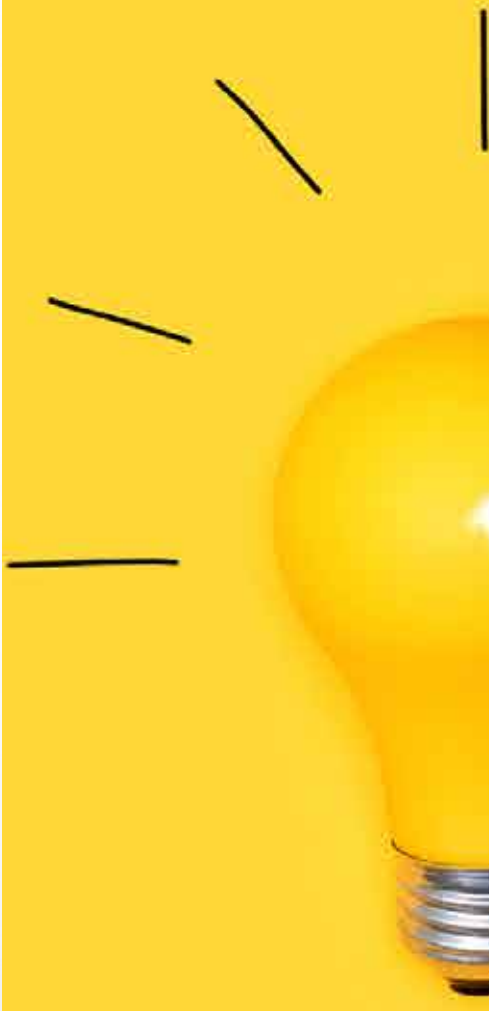
Because of the familiarity of courts with providing recourse for bodily injury in tort, these IoB cases are likely to result in new doctrinal lines of software liability. Instead, the tort arguments are likely to shift toward various possible calculations of damages and to what extent any liability protection exists for the device manufacturers—akin to traditional medical device harm cases.

In the case of product liability, if an IoT device fails and causes bodily harm or property damage, product liability litigation is likely to ensue. This will necessitate a reconsideration of more traditional product liability frameworks by the courts. For example, in assessing strict product liability, US courts have traditionally considered hardware to be a product and software to be a service (excluding software from strict-product-liability regimes).

As a matter of consistency, it is still unclear how the law will adapt in the context of the IoT.[62]

INTELLECTUAL PROPERTY LAW

Intellectual property refers to creations of the mind such as inventions, literary and artistic works, designs, symbols, names, images, etc. that are protected by law under different intellectual property rights such as patents, copyright, industrial designs, trademarks, or trade secrets, depending on the type of creation or work involved.[63] IoB devices are inventions that are protected by the Patent and Designs Act 2004. A patent is an exclusive right granted to the patent owner to decide who and how an invention is used by others. Although IoB devices are mainly protected under the Patent and Designs Act, some features of the invention are protected by other IP rights such as copyright, which protects the software, codes, and computer programmes used to set up the IoB device.[64] In addition, the three dimensional design of an IoB device and the name given to the particular device are protected by industrial designs and trademarks, respectively.[65] Trademarks generally protect brand names, logos, marks and signs used to distinguish one IoB device from another.[66]



LAW OF CONTRACT

The law of contract exists to govern the relationship between IoB inventors and users. It is not uncommon for IoB manufacturers to rely on end-user licence agreements to retain software rights. Even if the contracts have serious consequences, courts customarily uphold the majority of them.[67] Using the Internet of Things as a point of reference, we observe a collision between contract law from the sale of physical goods on the one hand and norms from the world of software contracts on the other.[68]

CRIMINAL LAW AND THIRD-PARTY DOCTRINE

Criminal litigation usually raises questions regarding the relationship between IoB EULAs and the human body. Precedent shows that prosecutors usually rely on the third-party doctrine and IoT data streams as models. However, direct interaction between IoB and criminal contexts has already begun, as evidenced by a recent insurance fraud prosecution that relied heavily on IoB-derived evidence. This insurance fraud prosecution case illustrates one aspect of the doctrinal and constitutional issues pertaining to the Fourth and Fifth Amendments that IoB raises in the US.[69] Similarly, in a 2017 case in the city of Ohio, where the prosecution accused the defendant of arson, the defendant's pacemaker was admitted into evidence. The Supreme Court in this case, stressed the need for the evolution of the third party doctrine to fit the dynamic nature of modern technologies.[70]

A DELICATE DANCE: THE CONUNDRUM OF BALANCING LEGAL ISSUES AND ADEQUACY IN THE INTERNET OF BODIES' LEGAL LANDSCAPE

The regulatory framework for IoB in Nigeria is still in its infancy. While there are several laws scattered across various legislations that may likely impact IoB, there is no single comprehensive legal framework that caters to the peculiarities of Internet of Bodies.

The increasing availability of the internet of bodies deepens the ethical grey area, and the law is currently not designed to keep pace with the steady progression toward the internet of bodies. The operation of the Internet of Bodies challenges the traditional concept of ownership, and users may gradually lose control over their IoB devices.[71]

In this context, the future necessitates striking a balance between the competing interests of appealing technological progress and vital human safety and privacy.[72]

As is typical with disruptive technology, legislation cannot keep up, and the IoB will not slow its progress in improving health management and improvements. As previously stated, the Internet of Things (IoT) offers an expanding range of devices that combine software, hardware, and communication capabilities to track personal health data, provide necessary medical treatment, or improve bodily comfort, function, health, or well-being.[73] While these benefits are appreciated, as are the general systems of the Internet of Things (IoT), these devices complicate an already complicated field riddled with legal, regulatory, and ethical risks, some of which we have already discussed. For example;

1. There is a dearth of proper regulation of standards of health devices by the National Agency for Food and Drug Administration and Control (NAFDAC). The NAFDAC has merely issued Guidelines for Registration of Medical Devices in Nigeria (2018), which does not address the standards of such devices but merely describes them to be any instrument, apparatus, or contrivance (including components, parts, and accessories thereof) manufactured, sold or advertised for internal or external use in the diagnosis, treatment, mitigation or prevention of any disease, disorder, abnormal physical state or the symptom thereof, in man or animal.[74]

2. The regulation of standards of products manufactured for, or brought into the Nigerian Market by the Standards Organisation of Nigeria (SON), is largely insufficient to address the external aspects of the IoBs as their specific needs may require, being products that are contrived for the preservation of life.

3. The protection of consumers against risks associated with using these products; some legal experts are calling for policies to protect consumers.[75]

4. There are no properly defined existing regulations on data brokers, and as such, data brokers can easily sell the personal information of their users to third parties.[76] On a positive note, with the Internet of Bodies, liability for breaches, bodily injury, or criminal activities is more easily identifiable since such harms are directly done to the human body.

IoB devices come in many forms such as wristwatch fitness monitors or pacemakers that transmit data about a patient's heart directly to a cardiologist, and are already widely used. The IoB envisions a world in which humans and objects communicate continuously over the internet or Bluetooth.

PRIVACY AND DATA PROTECTION

IoB devices are connected devices that monitor the human body, collect physiological biometric or behavioural data, and exchange information over a wireless or hybrid network.[77] IoB devices work with data, and the collection and use of personal data is central to their functionality. Wearable and home IoT devices frequently collect personal data, including biometric data such as voice and gait characteristics and personal preferences such as eating habits and preferred television programmes.

These devices and the data they collect can be utilised to provide consumers with great convenience and benefits. For instance, intelligent climate control systems can be remotely controlled, and fitness trackers can provide customised workout routines for their wearers.[78]

The quantity of personal data collected by IoB devices raises data protection concerns, such as who has access to the collected data and the safety of the data collection process. In addition, IoB introduces a more intimate relationship between humans and devices than IoT does. IoB devices monitor the human body, collect data and other personal information, and transmit it to the internet. The data collected and stored by these devices can be accessed without authorisation. For example, in 2018, a smart watch disclosed the location of a number of military facilities through a popular athlete's social network, Strava.[79] In addition, researchers were able to discover more data points from high level sensitive locations which identified more than 6,400 users.[80] The extent of intrusion led to the ban of internet-connected smartwatches in China in 2015.[81] IoB devices are inherently intrusive. This is due to the fact that they invade our bodies, pose significant risks to the integrity of our bodies, and result in a loss of control over our bodies, which may violate our body's autonomy and integrity.[82] Existing and future IoB devices can track, record, and store users' whereabouts, bodily functions, and what they see, hear, and even think.[83]

With such data being collected, it may be unclear who has access to it and how it is used. The data is stored in the cloud or on the device, where it may be vulnerable to unauthorised access.[84]

The data collection process can also pose an inherent risk to privacy, depending on what is being collected, how frequently it is collected, whether there is a determination of the appropriate lawful basis prior to collection, and whether individuals can easily opt-out of collection or prohibit companies from selling their data.[85] IoB devices can track users' locations as well as various body parameters such as cardiac rhythms, sleep patterns, and menstrual cycles. Parents also make use of cameras and sensor-based monitors to keep watch over their children's movements.[86] It is unclear whether consent is obtained during the collection process and whether users have the option to opt out of data collection or transfer at any time.

Another concern is the transfer of data retrieved by IoB devices and whether the data subject is aware of the transfer. Transparency about data processing is an issue with wearables.[87] According to research, insurance companies use patient data collected by Continuous Positive Airway Pressure (CPAP) machines used by people with sleep apnea to monitor compliance. As a result, if the device was not used for the required amount of time, the insurance company refused to pay for it.[88]

The biometric data captured by implantable cardiac devices could be used as evidence in disputable criminal cases, as it was in the famous Ross Compton lawsuit.[89] From the case of Ross Compton, it's unclear whether law enforcement's use of IoB data violates constitutional protections against self-incrimination and unreasonable search and seizure. In this case, officers used data from Compton's cardiac pacing devices to determine whether a critically ill man could escape a fire while neatly packing his belongings into a suitcase. Based on the pacemaker, which transmits data to a physician, the odds were stacked against him.

Amazon appears to be working on another arm motion tracker for warehouse workers.[90] With this device, Amazon would be able to detect idle employees and collect information such as the worker's location and hand movement. Although this device is intended to ensure employee productivity, it will give employers highly personal information about their workers, such as bathroom breaks.[91]

The possibility of these devices being hacked and health information being compromised is at the heart of data protection. This is an important debate because health data is sensitive personal data that, if compromised, can put data subjects at risk. This can lead to discrimination and stigma, which have been major concerns in the aftermath of health data breaches. There have been reports of people being denied insurance policies because of their health.[92] It has been documented that IoB testing kits that identify a person as a carrier of a genetic disease that could be passed on to their children result in insurance policy denials for those children.[93] There has also been a reported case of a person being incriminated in criminal activity based on health records retrieved from an IoB device.[94]

SECURITY RISKS OF IOB

The Internet of Bodies has resulted in remarkable technological advancements and benefits. However, its use does not come without attendant risks, particularly security risks. IoB is enabled by the internet and software programmes, which are supposedly vulnerable to breaches and malicious attacks. IoB devices are vulnerable to the same security threats as IoT devices or any other technology that stores data in the cloud or elsewhere, but the risk is higher due to the nature of IoB devices and the sensitive personal and/or health information they process.[95] The major concerns about the ecosystem in which IoB devices are used can be seen in the emerging trends of wearable, implanted, or ingested devices to improve health and/or lifestyle.[96] A physical device implanted in or attached to the body will communicate wirelessly with a monitoring device, such as a smartphone, which will then relay data to a cloud service.

Moreover, an external party may then gain access to the data. This assemblage of hardware and software, logical communication paths, and organisational boundaries introduces multiple layers of complexity, each of which is susceptible to failure, degradation, compromise, and attack.[97]

Some security risks may arise from flaws in software programmes, which can be exploited to steal or manipulate the information collected by the device, disrupt its operation, or otherwise cause it to behave in unexpected or unintended ways.[98] IoBs used in health facilities have been noted to run on outdated softwares, which increases the risk to healthcare facilities and patients.[99] Already, the number of attacks[100] against healthcare facilities is on the rise.[101] According to a 2022 report, the healthcare sector recorded the highest data breach cost for the twelfth year in a row.[102]

In 2020, a psychotherapy facility suffered a data breach in Finland that exposed health records of patients.[103] In the same year, a German healthcare facility suffered a ransomware attack that led to the death of a patient.[104]

Some of the security challenges prevalent in the use of IoB devices include;

1. **Cyberattacks**: IoB devices, as with other technological devices, are susceptible to cyber-

attacks. The aim of these attacks/hacks is to disable computers, interfere with the network, steal data, or use a breached computer system to launch additional attacks. Cybercriminals use different methods to launch a cyber attack, including malware, phishing, ransomware, man-in-the-middle attack, or other methods.[105] While cyber-attacks are not alien to technological systems, their consequences on IoB systems and devices are dire. The use of IoB has been a game-changer for people with specific medical conditions such as diabetes, cancer, asthma etc.[106] While there are no reported specific cyber attacks on IoB systems/devices within the health ecosystem, there have been reported cases of cyberattacks on health care systems.

According to data from the CyberPeace Institute,[107] the average cyberattack on a health care system leads to 19 days of patients being unable to receive treatment,[108] and where the patients' case is critical, it may cause death. For instance, the ransomware attack on Düsseldorf hospital prevented it from handling a patient's scheduled medical care at the hospital, which resulted in the death of the patient.[109] Another instance of a ransomware attack was in 2021. The CHwapi hospital in Belgium suffered a cyberattack that prompted the facility to redirect emergency patients to other hospitals and delay surgical procedures. staff and nurses were forced to abandon digital entries and turn to pen and paper for patient assessments because the threat actors used Windows BitLocker to encrypt CHwapi"s file and backup servers, although they hadn't stolen or leaked the data.[110]

2. **Exposure of sensitive information**: Another security challenge faced by IoB systems and devices is the exposure of the sensitive information of users or patients. For instance, between January 18 and February 24 2022, cybercriminals maintained unauthorised access inside ARcare's computer systems, reviewing and stealing sensitive individual information. On April 4, it was discovered that some stolen data was exposed on the internet. The information stolen included names, state ID numbers, financial account information, medical treatment, prescription, medical diagnosis, and health insurance information.[111] Also, in May 2020, Blackbaud, Trinity Health's third-party vendor responsible for storing a backup of its donor database, fell victim to a ransomware attack attempt.

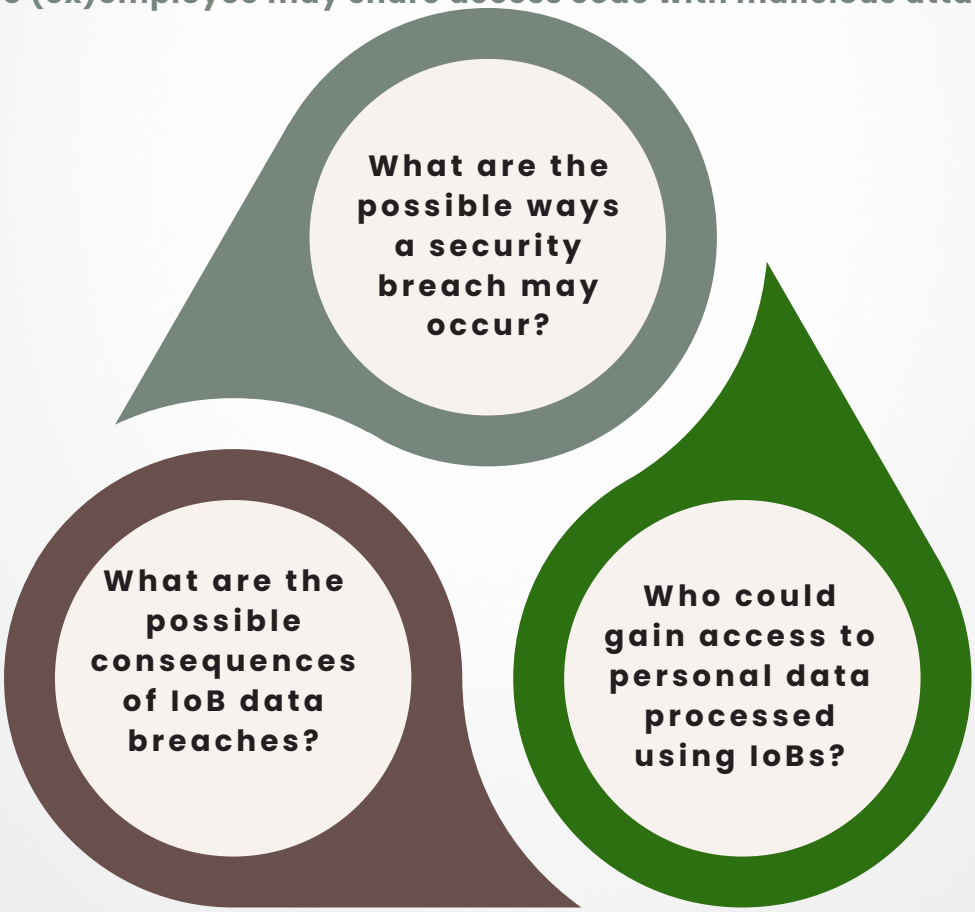
Trinity Health, with the support of forensic experts and law enforcement, was able to successfully block the ransomware attack attempt, but not before the hackers exfiltrated a subset of data that included information linked to Trinity Health.[112] This exposure of sensitive data may result in identity theft by malicious actors.

3. Surveillance and profiling: Biohackers can remotely eavesdrop, intercept, and even alter raw unencrypted data using high-gain antennas.[113] Nicole Lindsay, a technology researcher, describes this as a dystopian Orwellian state where IoB and its AI influence could create a dystopian Orwellian state where genetic anomalies can be edited or removed, behaviours can be tracked, and citizens can be constantly tracked.[114]

4. **National security issues**: The use of IoBs may, in processing aggregate data, expose security or classified information. A classic example is the Strava incident. The U.S. Department of Defense (DoD) had been encouraging health tracking devices in an effort to combat the obesity epidemic and conducted a program that gave out fitness trackers to more than 20,000 soldiers. The device was used to track the distance and time they exercised. However, it inadvertently exposed the locations of bases and important facilities based on where the geo-tracking stops. Strava, the American internet service focused on tracking physical exercise, later released a detailed and comprehensive map that exposed hidden military bases and camps of U.S. military and civilian personnel and the life patterns of service members, prompting the DoD to review.[115]

A summary of the possible means of a security breach and the consequences of using IoB can be seen in the diagram below.

- Mass vulnerability probing by a cyber attacker.
- Intercepting the cellular network by a cyber attacker.
- Employing reverse-engineering firmware
- Cyber attackers gaining network access through the information available on the dark web after the target system had suffered a previous hack.
- Employers, security researchers, or device manufacturers' security access code/token to the location of sensitive data may get into the hands of unauthorised persons.
- A rogue (ex)employee may share access code with malicious attackers.



- Death or physical harm as a result of the exposure of sensitive data.
- Global and national security issues.
- Identity theft.
- Unintended personal identification by government agencies.
- Negative profiling and possible loss of insurance premium.

- Hackers/malicious attackers
- Security researchers
- Employers & Employees
- Insurance companies
- Healthcare providers
- Device manufacturers
- Law enforcement agencies, government

RECOMMENDATIONS

• REGULATION

Aside from conferring obligations on entities, regulations also serve as a means to protect the rights of individuals.From our research, there is no comprehensive law that caters sufficiently to the peculiarities of IoB, which leaves entities with open-ended discretion on the system's appropriation and also puts users in the dark on several crucial issues. In addition, the rapid acceptance rate of the IoB marks it as one of the areas of technology and development that needs to be regulated. Hence it is recommended that a regulation that caters to the IoB be enacted. Key considerations for regulating IoB include the terms and conditions under which they can be used, the protection of vulnerable groups, containing surveillance, product liability, and the issue of privacy and security. In addition to the regulations, transparency and protection standards for the use and administration of IoB devices should be adopted. This should also include incorporating the right to opt out of data collection while using an IoB device.

In as much as new areas of threats, risks, and threats will continue to emerge, regulations might become almost stale as they emerge. Hence, it is recommended that laws and regulations be subject to constant review. In addition, effective regulation of the IoB will require multi-agency collaboration. Hence, it is recommended that regulatory agencies in consumer protection, health, data protection, information, and cybersecurity be actively involved in the regulation. However, there might be duplicity of function where the individual agencies regulate. Hence, countries can establish bodies that contain members of these agencies for the purpose of regulation.

• PRIVACY CONSIDERATIONS

The peculiarities of the IoB devices are such that large volumes of data can be collected and can be used for surveillance. Privacy recommendations for IoB include the following:

1. **Data Protection by Design and Default**: Data protection by design suggests that data protection should be embedded into the design specification of IoB devices. This means that data protection compliance should be a forethought in the development of these devices and clearly and carefully woven into its development so that these devices are automatically privacy conscious in the manner they collect and process data. Data protection by default encourages companies to maintain the highest privacy protection by default.

This means that only personal data necessary for specific purposes is processed for that purpose. Hence, companies manufacturing IoB devices should include as default settings the most privacy friendly combination of functions necessary to process data for a particular purpose,

2. **Data retention and storage**: Considering the large volume of data collected, there should be a need to set the retention schedule for all data collected. While some of these data can be subject to retention based on applicable laws, other data should be subjected to shorter retention periods. Data deletion options should also be embedded into the products.

3. **Data minimisation**: IoB can potentially collect more data than is needed, especially for devices inserted in the body or ingested, and those data can be collected in real-time. It is recommended that policies should stipulate usage only to data that is collected necessary for the purpose of processing should be stored, while other data should be deleted or encrypted and should be limited in access when they are stored. For the usage of these data, it is recommended that the users are properly informed of what it will be used for. Also, usage should be limited to the purpose disclosed.

4. **Stringent privacy considerations**: There should be more stringent privacy considerations to protect the data of vulnerable users such as children and vulnerable persons. By nature, children might not understand the full implications of using IoB devices.

However, an additional layer of caution will be to ensure parental consent and minimising the data collected, and disclosing how those data can be used. Furthermore, privacy-preserving solutions should be adopted for analytics and monitoring to avoid surveillance.

5. **Restriction on third-party access to data**: Most data collected by IoB can be categorised as sensitive data. Hence, it is recommended that such data should be shared with third parties only based on necessity. Also, the data collected should not be subjected to advertisements and should not be shared with third parties that do not provide joint services with the administrator of the data collected.

6. **Data Control by Users**: It is recommended that users should have considerable control over the kinds of data that will be collected per time. There should be shared control of data between the data subject and the administrators, especially for health data, such that the data subject can choose which data can be collected at different points in their usage of a device. Also, users should have blackout periods where the device might not be used at all and will not be collected. This may be more applicable to devices that are injected or have been implanted into the body.

7. **Conducting Data Protection Impact Assessments (DPIA)**: DPIAs afford product developers to assess all risks associated with using a product and how those risks can best be mitigated. At best, it provides reasonable insight into the privacy issues that users may encounter while using a product. Hence, it is recommended that DPIAs should be a matter of compulsion for all IoB devices and submission of DPIAs should be a part of the approval conditions for the market availability of such devices.

• SECURITY CONSIDERATIONS

The peculiarities of the IoB devices are such that large volumes of data can be collected and can be used for surveillance. Privacy recommendations for IoB include the following:

The dangers of wearable devices are such that the implications of cyberattacks can be life-threatening and can alter the behaviours of individuals. Hence, it is recommended that there should be cybersecurity guidelines that impose specific technical measures to ensure the safety of the devices while in use. These security measures include end-to-end encryption of data collected while the data is in transit or at rest.

It is further recommended that IoB administrators be subject to a constant audit process that examines new vulnerabilities in their systems, possible areas of threat, and the measures to address the threats identified.

Device manufacturers, healthcare facilities, and providers should invest in and implement authentication systems and mechanisms, monitor devices in real-time for detection, segment networks and protect each sub-network at its own level, and use appropriate security protocols. Healthcare facilities should also maintain an accurate inventory of connected devices. In addition, the implementation of the International Medical Device Regulators Forum's (IMDRF) Principles and Practices for Medical Device Cybersecurity provides useful guiding principles for third-party risk management, incident response, vulnerability assessments, and other pertinent security principles designed specifically for IoBs.[116]

CONCLUSION

The Internet of Bodies has pushed the frontiers of the Internet of Things and is snowballing in adoption. This research has analysed the nature of IoBs, their benefits across sectors, and the applicable laws to IoB. The research shows the inadequacy of the applicable laws to IoB and the regulatory gaps that currently exist in the applicable laws. Furthermore, the research addresses the security and data protection issues associated with IoB. The issues identified include the dire and possible life-threatening impact of a data breach, the possibility of third-party access, the volume of data collected, which could be essentially intrusive, and the actual knowledge of data subjects on all processing activities that happen on their data. Nevertheless, the recommendations reflect the need for a comprehensive regulatory framework and multi-stakeholder inclusion in establishing a regulatory body. The research also recommended data protection considerations, which include data minimisation, data retention considerations, having an appropriate lawful basis, data protection by design and default, and allowing for blackout periods to allow users to have more control over the data collected.

REFERENCES

1. Matt Zborg,'The Ten Hottest Medical Technologies - What to Know' (MTS16 May 2022) <https://www.medicaltechnologyschools.com/medical-lab-technician/top-new-health-technologies> accessed 5 January 2023.
2. Ibid
3. Nambiar, Kavya 'Internet of Bodies - Everything You Need to Know | Analytics Steps' https://www.analyticssteps.com/blogs/internet-bodies-everything-you-need-know . Accessed 6 November 2022.
4. Andrei Klunikin "What Is The Internet of Bodies (IoB), and Why Should You Care?" ITRex, 8 September 2022, https://itrexgroup.com/blog/internet-of-bodies-iob-definition-benefits-examples/.
5. Xiao Liu, 'The Internet of Bodies Is Here. This Is How It Will Change Our Lives' (World Economic Forum4 June 2020) <https://www.weforum.org/agenda/2020/06/internet-of-bodies-covid19-recovery-governance-health-data/> accessed 1 April 2023.
6. 'Tracking How Our Bodies Work Could Change Our Lives' (World Economic Forum) <https://www.weforum.org/agenda/2020/06/internet-of-bodies-covid19-recovery-governance-health-data/> accessed 11 January 2023
7. Monica, 'The Internet of Bodies Will Change Everything, for Better or Worse' 29 Oct. 2020, <https://www.rand.org/blog/articles/2020/10/the-internet-of-bodies-will-change-everything-for-better-or-worse.html> accessed 4 November 2022.
8. Nambiar (n 3).
9. Bernard Marr, 'What Is the Internet of Bodies? And How Is It Changing Our World? | Bernard Marr' (Bernard Marr2 July 2021) <https://bernardmarr.com/what-is-the-internet-of-bodies-and-how-is-it-changing-our-world/> accessed 1 April 2023.
10. 'IoT (II): From the Internet of Things to the Internet of Bodies | AEPD' (AEPD11 January 2021) <https://www.aepd.es/en/prensa-y-comunicacion/blog/iot-ii-from-iot-to-iob> accessed 1 April 2023.
11. Sailesh, Adithya. "Internet of Bodies - An Overview." IEEE LINK, 27 April 2020, https://medium.com/ieeekerala/internet-of-bodies-an-overview-9302579af62c.
12. Blog A, 'The Internet of Bodies Ends Bodily Autonomy' (Algora Blog, 31 August 2021) <https://www.algora.com/Algora_blog/2021/08/31/the-internet-of-bodies-ends-bodily-autonomy> accessed 11 January 2023
13. 'How Human Are You? The Internet of Bodies Is Here, but Are We Ready?' (Taylorwessing.com6 February 2023) <https://www.taylorwessing.com/en/interface/2023/iot---next-gen/how-human-are-you-the-internet-of-bodies-is-here-but-are-we-ready> accessed 1 April 2023.
14. Klunikin (n 4)
15. MobiDev, 'Meeting the Future: Internet of Bodies' (IoT For All17 February 2022) <https://www.iotforall.com/meeting-the-future-internet-of-bodies> accessed 1 April 2023.
16. What Is The Internet of Bodies (IoB), and Why Should You Care?' (ITRex, 8 September 2022) <https://itrexgroup.com/blog/internet-of-bodies-iob-definition-benefits-examples/> accessed 1 April 2023
17. ibid.
18. Amine Rghioui and others, 'An IoT Based Diabetic Patient Monitoring System Using Machine Learning and Node MCU' (2021) 1743 Journal of Physics: Conference Series <https://iopscience.iop.org/article/10.1088/1742-6596/1743/1/012035> accessed 1 April 2023.
19. Monica (n 7).
20. Kavya Nambiar, 'Internet of Bodies - Everything You Need to Know | Analytics Steps' <https://www.analyticssteps.com/blogs/internet-bodies-everything-you-need-know> accessed 15 November 2022.
21. ibid
22. Man's Pacemaker Data Used Against Him in Arson Case. https://www.cbsnews.com/news/mans-cardiac-pacemaker-data-led-to-arson-charges/. Accessed 7 November 2022.
23. 'Telltale Heart": Evidence Found in Defendant's Cardiac Pacemaker Contains Incriminating Evidence of Arson – Juris Magazine' <https://sites.law.duq.edu/juris/2017/04/02/telltale-heart-evidence-found-in-defendants-cardiac-pacemaker-contains-incriminating-evidence-of-arson/> accessed 16 January 2023 Pack L, 'Is Using Pacemaker Data "Stealing Personal Information"? Judge in Middletown Arson Case Says No' (journal-news) <https://www.journal-news.com/news/crime--law/using-pacemaker-data-stealing-personal-information-judge-middletown-arson-case-says/BAGH5WM0iCxOTwTPfM3P7J/> accessed 16 January 2023

24. Ibid.
25. Popescu VF, 'From Human Body Digitization to Internet of Bodies toward a New Dimension of Military Operations' (2019) 24 Land Forces Academy Review 242 <https://sciendo.com/article/10.2478/raft-2019-0029> accessed 1 April 2023
26. 'Smart Helmet in Applied Sciences' <https://encyclopedia.pub/entry/10761> accessed 1 April 2023
27. 'How Human Are You? The Internet of Bodies Is Here, but Are We Ready?' (6 February 2023) <https://www.taylorwessing.com/en/interface/2023/iot---next-gen/how-human-are-you-the-internet-of-bodies-is-here-but-are-we-ready> accessed 1 April 2023
28. Convercon, 'From Internet of Things to Internet of Bodies and Internet of Behavior.' (Convergence Consulting, 5 May 2022) <https://convercon.com/from-internet-of-things-to-internet-of-bodies-and-internet-of-behavior/> accessed 1 April 2023
29. Andrei Klunikin "What Is The Internet of Bodies (IoB), and Why Should You Care?" ITRex, 8 September 2022, available at <https://itrexgroup.com/blog/internet-of-bodies-iob-definition-benefits-examples/> accessed 2 November 2022.
30. Ibid.
31. Arvind Lakshminarayanan 'How the Internet of Things is Revolutionising Healthcare' (June 17, 2020) available at https://www.crayondata.com/how-the-internet-of-bodies-is-revolutionizing-healthcare/ accessed 2 November 2022.
32. Ibid.
33. Ibid.
34. A Klunikin (n 29)
35. Ibid.
36. Ibid.
37. Ibid.
38. A Klubnikin (n 29).
39. Convercon, 'From Internet of Things to Internet of Bodies and Internet of Behaviour' (5 May 2022) available at<https://convercon.com/from-internet-of-things-to-internet-of-bodies-and-internet-of-behavior/>accessed 2 November 2022.
40. A Klubnikin (n 29).
41. Ibid.
42. 1999 Constitution of the Federal Republic of Nigeria (as amended), S.33
43. Ibid. Section 34
44. Ibid. Section 37
45. Evidence Act 2011, Section.84
46. Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020, Article 2.4.
47. Medical and Dental Practitioners Act CAP M8 2004 LFN, S.1
48. Ibid, S.13 (3)
49. Ibid. S.13 (1)
50. Code of Medical Ethics
51. Code of Medical Ethics, S.19
52. Code of Medical Ethics, S.44
53. National Health Act 2014, Part II.
54. ibid
55. National Health Act 2014, section 27 and 28
56. Cybercrimes (Prohibition, Prevention, ETC.) Act 2015, Explanatory Memorandum
57. Cybercrimes (Prohibition, Prevention, ETC.) Act 2015, Explanatory Memorandum , section 58
58. National Agency for Food and Drug Administration and Control Act, S.31
59. The Nigerian Data Protection Regulation 2019 Ss. 2, &
60. Jenni Ryal 'How Your Smart Device Caused the Internet to Crash and Burn', MASHABLE (Oct. 21, 2016), <https://mashable.com/2016/10/21/dyn-attack-iot-device/> accessed 5 November 2022.
61. Ibid
62. Dentons, Carlson S., Snider C., 'Connected Living and IoT Litigation – Product liability, consumer protection, privacy and other legal issues: An American and Canadian comparative perspective' (February 18 2020)
63. 'What Is Intellectual Property (IP)?' <https://www.wipo.int/about-ip/en/index.html> accessed 14 April 2023.
64. Copyright Act 2022, section 108.
65. Patent and Designs Act, section 12 and Trademarks Act 2004, section 9.
66. Ibid.
67. Matwyshyn A. M. 'The Internet of Bodies' (1 January 2021) <https://papers.ssrn.com/abstract=3452891> accessed 5 November 2022

68. Ibid
69. Matwyshyn Pg. 72
70. Ibid
71. ibid.
72. El-Khoury and Arikan 'From the internet of things toward the internet of bodies: Ethical and legal considerations' (10 May 2021)
<Moufid El-Khoury_https://doi.org/10.1002/jsc.2411> accessed on 4th November, 2022.
73.Shiraz Ali Wagan and others, 'Internet of Medical Things and Trending Converged Technologies: A Comprehensive Review on Real-Time Applications' (2022) 34 Journal of King Saud University - Computer and Information Sciences 9228 <https://www.sciencedirect.com/science/article/pii/S1319157822003263> accessed 12 April 2023.
74. CAP N1 Laws, Art. 31.
75. Lee et al. The Internet of Bodies: Opportunities, Risks and Governance. https://www.rand.org/pubs/research_reports/RR3226.html accessed on 4th November, 2022.
76. Allyson Young Blood 'The Internet of Bodies will Change Everything for Better or Worse', Rand Corporation (October 29 2020) Rand Corporation <https://www.rand.org/blog/articles/2020/10/the-internet-of-bodies-will-change-everything-for-better-or-worse.> accessed 5 November 2022.
77. Convercon, 'From Internet of Things to Internet of Bodies and Internet of Behaviour' (5 May 2022) available at<https://convercon.com/from-internet-of-things-to-internet-of-bodies-and-internet-of-behavior/>accessed 2 November 2022.
78. Office of the Victorian Information Commissioner (OVIC) ' Internet of Things and Privacy-Issues and Challenges' available at <https://ovic.vic.gov.au/privacy/resources-for-organisations/internet-of-things-and-privacy-issues-and-challenges> accessed 6 November 2022.
79. Jeremy Hsu, 'Strava Data Heat Maps Expose Military Base Locations around the World' (WIRED30 January 2018) <https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/> accessed 14 April 2023.
80. Zack Whittaker, 'Fitness App Polar Exposed Locations of Spies and Military Personnel' (ZDNET8 July 2018) <https://www.zdnet.com/article/fitness-app-polar-exposed-locations-of-spies-and-military-personnel/> accessed 14 April 2023.
81. BBC News, 'China Imposes Smartwatch and Wearable Tech Army Ban' (BBC News13 May 2015) <https://www.bbc.com/news/technology-32718266> accessed 14 April 2023.
82. United Nations Population Fund, 'State of World Population 2021 Report' (2021) https://www.unfpa.org/sites/default/files/pub-pdf/SoWP2021_Report_-_EN_web.3.21_0.pdf accessed 14 April 2023.
83. Monica (n 7)
84. 'B3 Data Security' (Ncsc.gov.uk2023) <https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/b-3-data-security> accessed 14 April 2023.
85. Ibid.
86. A Klubnikin (n 29)
87. Vidhi Kapoor and others, 'Privacy Issues in Wearable Technology: An Intrinsic Review' [2020] SSRN Electronic Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3566918> accessed 14 April 2023.
88. Lee, Boudreaux, Chaturvedi et al, 'The Internet of Bodies, Opportunities, Risks and Governance' Rand Corporation (2020) available at <https://www.rand.org/pubs/research_reports/RR3226.html> accessed 3 November 2022.
89. Ibid
90. Monica, 'The Internet of Bodies Will Change Everything, for Better or Worse' 29 Oct. 2020, <https://www.rand.org/blog/articles/2020/10/the-internet-of-bodies-will-change-everything-for-better-or-worse.html> accessed 17 January 2023.
91. Ibid.
92. Lee, Boudreaux, Chaturvedi et al, 'The Internet of Bodies, Opportunities, Risks and Governance' Rand Corporation (2020) available at <https://www.rand.org/pubs/research_reports/RR3226.html> accessed 3 November 2022.
93. Ibid.
94. Lee, Boudreaux, Chaturvedi et al (n 92).
95. Convercon (n 38)
96. Das AK, Zeadally S and Wazid M, 'Lightweight Authentication Protocols for Wearable Devices' (2017) 63 Computers & Electrical Engineering 196 <https://www.sciencedirect.com/science/article/pii/S0045790617305347> accessed on 4 November, 2022.
97. Lee, Boudreaux, Chaturvedi, Romanosky, Downing, 'The Internet of Bodies: Opportunities, Risks and Governance', Rand Corporation, https://www.rand.org/content/dam/rand/pubs/research_reports/RR3200/RR3226/RAND_RR3226.pdf

accessed on 4 November, 2022.
98. Ibid.
99. Sergiu Gatlan, 'Medical IoT Devices with Outdated Operating Systems Exposed to Hacking' (BleepingComputer11 March 2019) <https://www.bleepingcomputer.com/news/security/medical-iot-devices-with-outdated-operating-systems-exposed-to-hacking/> accessed 14 April 2023.
100. 'Rise in Cyber Attacks on Healthcare Institutions Increases Patient Mortality' (Cynerio.com2020) <https://www.cynerio.com/blog/rise-in-cyber-attacks-on-healthcare-institutions-increases-patient-mortality> accessed 14 April 2023.
101. 'The Mounting Death Toll of Hospital Cyberattacks' (POLITICO28 December 2022) <> accessed 14 April 2023.
102. IBM, 'Cost of Data Breach Report, 2022' (n.d.) https://www.ibm.com/downloads/cas/3R8N1DZJ accessed 14 April 2023.
103. William Ralston, 'They Told Their Therapists Everything. Hackers Leaked It All' (WIRED4 May 2021) <https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/> accessed 14 April 2023.
104. William Ralston, 'The Untold Story of a Cyberattack, a Hospital and a Dying Woman' (WIRED UK11 November 2020) <https://www.wired.co.uk/article/ransomware-hospital-death-germany> accessed 14 April 2023.
105. 'What Is a Cyber Attack? | Cyber Attack Definition' (29 June 2021) <https://www.unisys.com/glossary/what-is-cyber-attack/> accessed 18 January 2023.
106. 'The Internet of Bodies (IoB) and It's Impact on Today's Healthcare' <https://www.linkedin.com/pulse/internet-bodies-iob-its-impact-todays-healthcare-jamie-allan> accessed 18 January 2023.
107. 'Cyber Incident Tracer #HEALTH' (Cyber Incident Tracer #HEALTH) <https://cit.cyberpeaceinstitute.org/> accessed 18 January 2023.
108. Miller M, 'The Mounting Death Toll of Hospital Cyberattacks' (POLITICO) <https://www.politico.com/news/2022/12/28/cyberattacks-u-s-hospitals-00075638> accessed 18 January 2023
109. 'A Patient Has Died after Ransomware Hackers Hit a German Hospital' (MIT Technology Review) <https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/> accessed 18 January 2023.
110. Belgian Hospital Reroutes Critical Patients after Cyberattack' (Hot for Security) <https://www.bitdefender.com/blog/hotforsecurity/belgian-hospital-reroutes-critical-patients-after-cyberattack/> accessed 18 January 2023.
111. 'Notice of Security Event'<https://www.arcare.net/wp-content/themes/altitude-pro/security_notice.html> accessed 20 January 2023.
112. '14 Biggest Healthcare Data Breaches [Updated 2023] | UpGuard' <https://www.upguard.com/blog/biggest-data-breaches-in-healthcare> accessed 20 January 2023.
113. Ibid.
114. Nicole Lindsey, "Internet of Bodies: The Privacy and Security Implications" <https://www.cpomagazine.com/data-privacy/internet-of-bodies-the-privacy-and-security-implications/> accessed 28 November 2022
115. Copp T, 'Fitbits and Fitness-Tracking Devices Banned for Deployed Troops' (Military Times, 7 August 2018) <https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/> accessed on 7th November 2022.
116. International Medical Device Regulators Forum, 'Principles of Medical Device Cybersecurity: Pre-Market Expectations and Post-Market Management' (18 March 2020) https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf accessed 14 April 2023.