Quest Journals
Journal of Research in Business and Management
Volume 10 ~ Issue 6 (2022) pp: 45-57
ISSN(Online):2347-3002
www.questjournals.org

Research Paper

The Internet of Things Devices: Challenges for Product Liability Law

Olowokere Emmanuel Nimbe
(Business Administration Department, the Federal University of Technology)

Abstract: *One of the subsets of Technology today is the Internet of Things (IoT). The number of so-called smart connected consumer products is increasing and the IoT market expanding.While IoT brings a host of benefits to the consumers, it also brings a set of product safety and liability issues that are unique to the autonomous and interconnected nature of IoT. With the spread of IoT, threats to security increasingly stem not only from cyber-attacks on providers of online services but also from the exploitation of vulnerabilities in commonly-used consumer products.The paper aims to present challenges posed by IoT that need to be addressed by product liability law. In the IoT era, liabilitylaw is faced with some challenges which make it difficult to identify the root cause of product failures.The considerations and potential concerns about consumer product safety in the IoT era are evolving in Nigeria. This discourse will promote discussion about consumer product safety during the still relatively early stages of the connected devices in the country, rather than wait until incidents and injuries force the discussion.*

Keywords: *consumer, Internet of Things,safety, products liability law*

Received 26 May, 2022; Revised 05 June, 2022; Accepted 08 June, 2022 © The author(s) 2022. Published with open access at ***www.questjournals.org***

I. INTRODUCTION

The Internet has remained the most sophisticated and rapidly growing technology man has ever invented. The invention impacts on all aspects of human activities. It has dramatically changed how human beings work, live, play, think, and make decisions in a very short time. Previously, the Internet only connected computers, servers and mobile devices together in a network, meaning that people could connect to information across the globe. Today, numerous objects, devices and appliances, not typically associated with having communications capabilities can be connected to that same Internet and to each other – things like lightbulbs, cars, public transport, medical devices, manufacturing components, electricity meters, household appliances or home security systems. The IoT is an inevitable and radical progression of the connectivity made possible by the Internet.

Many authors have been trying to define the IoT phenomenon by expanding the concepts of "Internet" and "things", describing their features, ways of connecting and interacting. Rob van Kranenburg[23] explores and systematizes different definitions of the concept. One of them, given by the EU project Casagras, explains in details that:

IoT is a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.

The Organization for Economic Co-Operation and Development (OECD, 2018) refers to IoT as “an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world” [39]. The ever-expanding ecology of everyday objects with electronic interconnections is commonly referred to as “the Internet of Things” (IoT) [59]. Put simply, IoT is the connection of devices to the internet; it involves the use of sensor enabled devices designed to collect data about their environment, which frequently includes data related to people. For these devices to be “smart,” they must also generate, send, and receive data with minimal human interactions. These products include watches, glasses, health indicators, home automation, thermostats, fridges, and autonomous vehicles.Connected 'smart' cities have continued to shape the industry across many sectors, thus generating massive data fed into analytics to understand consumer behaviour.

The first IoT device has been attributed to the Carnegie Melon Computer Science Department [18]. In 1982, students connected a Coca-Cola vending machine to the school's Internet network which allowed them to remotely monitor whether the machine had any soda and the temperature the machine was running [18]. This started the IoT tradition of connecting non-computing devices to networks to start making people's lives easier. The term "Internet of Things" was not coined until much later in 1999 by Kevin Ashton of the Massachusetts Institute of Technologyin explaining how Internet-connected devices can change our lives [61]. Gubbi*et al.*[14] observe that IoT originated as a vision to interconnect various everyday objects through the internet to achieve a common goal. The idea of IoT is the connection of internet devices through which person can interact with the physical and digital world.

The IoT has the potential to deliver significant benefits to consumers. One of the more obvious benefits is that IoT-enabled devices and applications make consumers' lives easier and less prone to risk, and aim to promote efficiency and sustainability. Smart appliances in consumers' homes can help maximize productivity by allowing automation and coordination of menial tasks that otherwise require hours of manual labour. The ability of manufacturers to remotely modify IoT devices and applications means that these products have the potential to be upgraded even after they are acquired by consumers. For this reason, the IoT devices may gain improved performance or even entirely new features over the course of its life in the consumer's home [37]. There are also benefits to IoT-connected devices and applications that have the potential to make them safer to use. A feature of being connected to the IoT is that such a product can warn responsible parties about unsafe conditions and permit these problems to be addressed before a negative outcome occurs. Car seat sensors working via Bluetooth may, for example, be used to prevent parents from leaving their children on their own in a car, through an alert via their smartphone. If the problem is severe or cannot be rectified remotely, manufacturers can also initiate recalls in a timely and effective manner. Thus, an IoT device may be remotely monitored by the manufacturer or a third party for problems. Then, if a problem arises, the consumer can be notified immediately of the issue and, if necessary and possible, the device's software could be updated or patched. And if the device cannot be fixed remotely, the product could be recalled.Using IoT devices also opens up new avenues for innovation. Unlike traditional computation, which can only gather information from one's phone, tablet, or computer, IoT devices can theoretically collect information on everything. The data collected by IoT devices, in turn, can fuel further innovation. Combined with new machine learning techniques, these data can be used to improve self-driving cars, better diagnose health issues, save the environment, and provide other benefits that one cannot yet imagine[4]. Security and safety are other examples of IoT's benefits. Houses and other buildings can also be monitored and controlled to detect and prevent theft and other dangerous activities. IoT can also be deployed to manage traffic and reduce accidents[50].Consumer IoT-enabled devices for convenience still come with their share of risks and will inevitably result in product liability claims.

Product liability plays an indispensable role in safeguarding consumer rights. It provides helpful perspective on how law must adapt to the changes of a society more connected than ever before through the Internet. It raises challenges that have historical antecedents and others that require reinvention. It also taps into the value of a common-law system capable, if properly utilized, of advancing as technology does with increasing rapidity. There is currently enough growth to warrant a closer analysis of this potentially disruptive phenomenon on the impact of the proliferation of consumer IoT devices on product liability. A 2015 McKinsey Report estimated that "there are more than nine billion connected devices around the world, including smartphones and computers," and that by 2025 there may be somewhere between twenty-five to fifty billion such devices [29].Others predict that there will be more than one trillion IoT devices by 2025[5].Under the current legal landscape, consumers can hold manufacturers accountable for any damages incurred from using faulty products. However, new Internet-connected products, threaten to undermine product liability protections.Consumers all over the world are fast becoming part of the connected world, for reason that everyday devices such as mobile phones, home kit appliances, smart systems and wearable gadgets have become commonplace and interoperable. This paper focuses on IoT-enabled Consumer devicesrather than industrial IoT systems. This subset of IoT devices represents a significant percentage of the IoT ecosystem: it is estimated to have an economic impact of $370 billion to $1.9 trillion per year by 2025[29]. The work aims to present an understanding of product liability in the era of IoT. As the article considers IoT product safety hazards toconsumers, it examinesthechallenges that need to be addressed by product liability law.

II. OVERVIEW OF GLOBAL CONSUMER IOT MARKET

The increase in internet penetration by consumers and growing adoption of smart devices is likely to fuel growth of the global Consumer IoT market. Sonar Trend Platform has stated that the IoT market is driven primarily by technological innovations. On the other hand, changes in the lifestyle of today's society are also driving developments in the IoT sector. Digitalisation and the smartphone revolution have led to evermore compact, low-cost processing power, in addition to cheaper but more sophisticated sensors and cameras as well as ubiquitous wireless connectivity. Advances in machine and deep learning are propelling the development of intelligent self-learning systems. The expected gains due to automation and improved data-driven insights are immense and will further drive progress in this area as well as within IoT. Bluetooth, 5G, LiFi, NB-IoT or LoRa are just a range of new evermore present network technologies promising better and more network coverage, in addition to longer range and more energy efficient connectivity. Decreasing costs for memory and storage solutions are enabling the collection of big data, as well as subsequent data analytics services. Around 53% of the global population is connected to the internet, leveraging digital technologies many times daily to manage their lives [49].

The IoT is growing rapidly due to the increasing processing capacity of ever-smaller circuits. In 2015, there was an installed base of 15.4 billion IoT devices [46].while the world population was 7.3 billion people [55].A survey by networking equipment company Cisco estimates that 25 billion devices will be connected in the Internet of Things by 2015, rising to 50 billion by 2020 [7]. Gartner's more widely cited estimates give a more conservative prediction of 25 billion "things" being connected to the Internet by 2020. 27 billion devices have been connected over IoT in 2017. This number is expected to increase to 125 billion by 2030. The IoT market was already a $170 billion market by 2017. It is expected to grow to around $561 billion by 2022 [49]. Vehicular IoT applications and smart home devices are gaining traction; while in the public sector, municipalities are adopting IoT for intelligent transportation and public safety enhancements [1].These increased connections will lead to new innovations, resulting in $19 trillion worth of savings over the next ten years. By 2025, the value of these devices and the ecosystem they operate in is estimated to exceed four trillion dollars per year [29]. IoT devices are not only expanding in number and increasing in value to the economy, but also diversifying in kind. More and more, manufacturers are experimenting with different types of devices to connect to the IoT.

North America is expected to be a prominent market, owing to the growing role of IoT among the significant revenue-generating end-user industries of the region, driven by the deployment of connected cars, smart energy projects, home automation, and focus on smart manufacturing. In addition, rapid digitalization across industry verticals and technological advancements has further fueled the growth of IoT in this region. Moreover, the region has a strong foothold of IoT vendors, which contributes to the growth of the market. Some of them include IBM Corporation, Microsoft Corporation, Intel Corporation, Cisco Systems, Inc., and Google Inc, among others. In February 2020, Cisco announced enhancements to its IoT portfolio that enable service provider partners provide optimized management of cellular IoT environments and new 5G use-cases. New wireless technologies such as 5G, Wi-Fi 6 would lead to more devices and new IIoT use cases and would give service providers the tools to create competitive cellular IoT offerings for their customers. Machine-to-machine connections are anticipated to rise 19% and account for 50% of all connections by 2023, according to Cisco's 2020 Annual Internet Report [45].

Another primary market in the region is the home automation systems. The products consumers are looking to add to their homes include connected cameras (highest demand), video doorbells, connected light bulbs, smart locks, and smart speakers. According to a study at Stanford University and Avast, North American homes have the highest density of IoT devices of any region in the world. Notably, 66% of homes in the region have at least one IoT device. Also, 25% of North American homes boast more than two devices. The average household in the region would have an average of 9 devices by 2022, and nearly half (48%) of total devices and connections will be video capable.[45]Transparency Market Research, 2018 predicts that the consumer IoT market is likely to witness significant growth owing to growing adoption during the course of forecast period from 2018 till 2026. On the basis of application, home automation is likely to account for maximum market share in the global consumer IoT market. This is due to growing demand home monitoring in remote location and rising adoption of home automation device in various applications.

The global IoT market is expected to reach a value of USD 1,386.06 billion by 2026 from USD 761.4 billion in 2020 at a CAGR of 10.53%, during the period 2021-2026. With the development**,**of wireless networking technologies, the emergence of advanced data analytics, a reduction in the cost of connected devices, and an increase in cloud platform adoption, the market is expected to grow at a positive rate [45].Even if these projections of the impact of the Internet of Things turn out to be outlandish,the increasing role that IoT will play in our society cannot still be ignored. The Internet of Things is not science fiction—the ever decreasing costs of computational power and network connectivity are bringing many IoT products to market. Consumers are constantly surrounded by IoT devices like the Apple Watch, Nest home appliances, Samsung Smart TV's, 4G-connected Chevy cars, and more [4]. Many major corporations and organizations have their own vision of what the future of IoT should look like, and are racing to bring their visions to market before they are shut out by their competitors.

III. UNDERSTANDING PRODUCT LIABILITY

Product liability refers to defect-based tort cause of action under which a commercial seller can be held liable for selling a product with a dangerous defect. The broader definition loosens the defect-based constraint and includes anyground on which a seller might be held liable for the injuries that its product causes [4].Product liability refers to the area of law where manufacturers and retailers are held responsiblefor the damages caused by their products failures. Under the existing liability regime, productliability claims fall into three categories: negligence, strict liability, and breach of warranty. Negligence-based liability makes a product manufacturer responsible for damages if they produce defective products because they did not exercise the level of care that someone of ordinary prudence would have exercised under the same circumstances [4]. Strict liability, on the other hand, holds corporations responsible for the damages caused by their products, regardless of culpability. To be held strictly liable for damages, a producer's product must have manufacturing defects that proximately caused (proximate cause) the damages, and the producer must have failed to warn the user of the potential for damages. Breach of warranty cases are those that involve the manufacturers violating the implicit or expressed warranties of a product[4].

According to Goldberg and Zipursky, product liability is certainly imperfect: "liability law is expensive and in some ways unpredictable. On occasion, judges and jurors mishandle scientific information, display insensitivity to businessrealities, are harsh in their judgments about victim behaviour, and issue indefensible judgmentsabout liability and damages" [13]. Despite these drawbacks, product liability has some irreplaceable benefits. Product liability plays an important role in the society. It upholds fundamental understanding of fairness and also serves to keep products safer.Indeed, by raising the costs of selling dangerous merchandise, product liability incentivizescompanies to create safer appliances. John Goldberg andBenjamin Zipursky state that the case for product liability is incredibly easy:

"It holds manufacturers accountable to persons victimized by their wrongful conduct. Itempowers certain injured victims to invoke the law and the apparatus of governmentto vindicate important interests of theirs. It instantiates notions of equality before the lawand articulates and reinforces norms of responsibility. And in doing all these things, itcontributes in direct and indirect ways to deterrence and provides welfare-enhancingcompensation. For all these reasons and others, it is extremely valuable that courts, at thebehest of victims, have the authority to order commercial sellers of defective products that cause injury to compensate their victims" [13].

Additionally, the effectiveness of market forces is dependent on the existence of product liability. Indeed, individual or large class action suits often attract enough media attention toinform consumers about the potential dangers posed by a product.

IV. IOT-ENABLED CONSUMER PRODUCTS

In recent years, a growing range of IoT-enabled consumer products has been commercialised, penetrating many consumer product sectors and driving consumers' interactions with products in their everyday life. A 2014 Goldman Sachs report identified five key IoT areas of adoption: Wearables, connected cars, connected homes, connected cities and industrial Internet (including transportation, health care, oil and gas). For the purpose of this work, wearable technology, health monitors and implantable devices, smart-home products, toys and childcare equipment, andconnected automobiles are considered.

Described as the most important IoT product category [56],wearable technology refers to those devices that are worn by a user and are connected to the internet, often using a Bluetooth connection to the user's mobile device. The most common examples of wearable technology include smart watches and fitness trackers. While these devices do tell time or count steps, or sometimes both, they also can alert consumers to incoming calls and texts, notify of upcoming calendar appointments, monitor heart rate while you exercising, and track consumer using GPS. Fitbit, Garmin, Polar, Apple and others have had varying degrees of success with these smart watches and fitness trackers.

Implantable technology primarily consists of medical devices such as cardiac monitors, glucose sensors, and cochlear implants to improve hearing. These medical devices are used to monitor and treat chronic medical conditions. Health monitors allow consumers with serious medical conditions to work with their physicians to manage their ailments, or improve disease prevention [12]. There are devices that are ingested by or implanted directly into consumers. These devices are being developed primarily for monitoring chronic health conditions like diabetes and heart disease. They can also be used to detect accidents, fits, seizures, or heart attacks and alert emergency services. Furthermore, such devices can gather information about medication-taking, activity, and sleep patterns of patients, as well as measure blood pressure, glucose levels, and heart rates [37]. These devices greatly assist physicians in developing and tailoring treatment plans for their patients and also help ensure that urgent-care facilities are reserved only for true emergencies [37]. The benefits of this technology are obvious. It allows for real-time observation by medical professionals, which makes patients safer and reduces the need for long visits to the doctor's office. But internet-based monitoring also may come with some risks that the statute attempts to address. For example, as the device is connected to the internet, it may be vulnerable to unauthorized access. A software defect could potentially misread data, corrupt information, or even cause the device to malfunction.

An important and diverse category of IoT devices and applications is in the home setting. These devices include smart thermostats that can track energy usage and patterns; smart home appliances that can regulate operations remotely (like ovens that consumers may turn on before arriving home); smart locks and other security systems; sensors to detect flooding, smoke, or carbon dioxide; smart televisions; and “home hubs” that are themselves connected and can provide information to consumers, but can also permit consumers to control through voice commands other home IoT devices like smart lighting, security systems, smart thermostats, and smart high definition televisions. The “smart home” is a rapidly-developing sector in the IoT, and is significant from a product safety policy perspective as it brings “traditional” household products into this area of new technology. As everyday products are developed with technologies that allow them to be “connected” and their functions affected by external inputs, the management of the safety of those products becomes more complicated, and may raise new issues from a policy perspective. The smart home is known to be at the forefront of innovation regarding IoT monitoring and control systems. The primary value propositions are family and property protection and energy savings. For example, the Verizon Home Monitoring and Control network uses a wireless communications technology designed specifically for remote control applications in home automation. IoT-enabled home appliances and devices can be monitored and controlled outside the user’s home through a computer, tablet, or smartphone. The Verizon Home Monitoring and Control network allows users to adjust the lights, control the climate, manage the security system, receive automatic event notifications, and even lock and unlock doors.

A 2018 survey of 3,750 consumers by Ofcom [40] found that the most common connected devices in the UK include smartphones – used by 78% of respondents; smart TVs – in 42% of households surveyed; wearable devices – in 20% of households, including fitness trackers that monitor factors such as physical activity and location; smart speakers – in 13% of households, which can react to voice commands and be used to control other devices. Other applications for connected devices include home monitoring systems (such as those for heating systems, lighting systems, burglar alarms and cameras) and smart appliances such as kettles and fridges. These can often be remotely monitored or controlled by users for greater convenience or security. A 2018 survey of 1,000 consumers by the trade body techUK found that ownership of these products is growing more slowly than for the most prevalent devices stated above. Consumers most often cited cost as the main barrier to purchasing devices (41%), followed by privacy (21%) and cyber security concerns (16%) [53].

In an effort to cash in on children’s love of technology, a number of toy manufacturers are now developing and selling smart toys. The category of toys and childcare equipmentcovers both devices used by children for play, and devices used by theirparents to monitor their safety and health.Children’s toys on the market include varieties of dolls and toy creatures that can change children’s behaviour in order to entertain (such as by remembering answers given by a child, knowing what time it is or giving a weather forecast, and otherwise adapting to the child’s responses); construction games permitting children tobuild programmable gadgets; and specially-designed tablets that have various features permitting children to interact with their environment in different ways (including by uploading photos and documents to personalise) [54]. More complex and advanced products are being developed. For example, 3D printers designed to enable a child to make their own simple toys in the home are already on the market, with further development of this technology likely. Childcare equipment, such as baby monitor trackers send parents information about their baby’s vitals to their smartphone. Toys, such as those that are based on voice and/or image recognition (e.g. Hello Barbie, which is an Internet-connected version of the doll that has real conversations with kids) or app-enabled robots, and other mechanical toys are IoT-enabled consumer products. There are also devices that monitor children’s safety and health. Some of these devices are simply cameras or microphones connected to the internet for remote monitoring purposes. Others may provide more information, such as a toy containing a sensor that simultaneously relays to the parents information about the child’s location, body temperature, and heart rate. Another example is a child car seat that contains sensors to alert parents to their child’s physical condition, in the event the child is alone in a car and potentially overheating.

Some of these toys use Bluetooth connections to connect to a mobile device, and others record and store the parents’ and child’s information on the manufacturer’s computer system. Data protection and privacy concerns regarding a child’s personal data (i.e. who uses it, and who has access to it, and for what purpose) may be more sensitive, particularly where a child may be less aware of the risks of sharing certain personal data online. These considerations may have genuine safety implications, as well as raising privacy concerns. As with other online technology, these toys and their computer systems can fail or be compromised.

Automobiles are increasingly being connected to the internet, for such reasons as providing warnings to drivers of dangerous weather or road conditions, offering real-time diagnostics on the car’s condition, and even permitting the vehicle to be operated remotely or autonomously [37].. Technologies are also being developed and commercialised that enable a consumer's vehicle to connect with other devices, including with home-based technologies. For example, technology is being commercialised that allows users to control smart home products from their vehicles e.g. triggering custom routine actions (such as dimming lights or lowering the thermostat), showing the status of smoke or security alarms, and causing the garage door to open as the driversmove near their homes. The IoT is also used to monitor and control various components in cars. Ford and Intel teamed up in 2014 to explore new opportunities to personalize the user experience using facial recognition software and a mobile phone app. The joint research project, called Mobile Interior Imaging, incorporates perceptual computing technology to offer improved privacy controls and to identify different drivers and automatically adjust features based on an individual's preferences. The in-car experience is then personalized further by displaying information specific to the driver, such as his/her calendar, music, and contacts.

The advanced wireless features that make connected transportation technologies possible also present serious safety risks if they malfunction or are accessed by hackers. Researchers have demonstrated it is possible for hackers to obtain functional control over the operation of a vehicle or airplane through connected technologies. They have demonstrated the ability to remotely shut down engines, disable brakes, control steering, lock doors, and use turn signals in connected vehicles [43].For example, white hat hackers conducted a test where they hacked a Jeep Cherokee driving seventy miles per hour in downtown St. Louis, Missouri and cut the transmission so that the test driver could not accelerate by pressing the gas pedal [3].A "white hat" hacker generally refers to security researchers or other hackers who notify a vendor or other responsible party when they discover software vulnerability [22].While there are some autonomous cars on the roads in some countries, the vast majority of cars are still 'manned' vehicles. Autonomous cars are rare on Nigerian roads. When a crash occurs between two 'manned' cars due to driver error, the ultimate allocation of fault is normally an analysis of "who" was at fault. Autonomous or self-driving cars are becoming more and more prevalent. The emergence of a brand new and paradigm shifting technology (autonomous or self-driving car) has the potential to complicate how to assign blame and compensate the injured when, inevitably, something goes wrong.

V. IOT DEPLOYMENT AND APPLICATIONS IN SOME AFRICAN COUNTRIES

The emergence of Internet of Things is a global wave and IoT can be explained as a pervasive technology using connectivity of people and things now entering Africa as a continent from western world. African countries have taken advantage of the IoT technology in different sectors and already seeing tremendous growth in these sectors. A worthy example is the finance sector where virtually all customers have the banking applications on their electronic devices and can do banking transactions, irrespective of location. With cloud computing and new technologies in computing world, it is seen as a big driver in economy development. IoT has a lot of expected possible solutions that can be offered to individuals and organizations across Africa, which can provide answers to high relative poverty, security concerns, illiteracy and poor basic amenities to half of the continent population. Despite Africa backwardness in certain technology, some African countries have taken steps to be leading users or deplorers of IoT in their infrastructure. The countries have seen tremendous growth in those areas where IoT were being deployed.

With about 48 million active internet users, Nigeria is one of African countries with an enormous market for IoT. Nigeria has been building the infrastructure slowly from the year 2010 when it formulated national information communication technology strategic plan 2010-2015. Like many countries in Africa, while Nigeria is yet to establish major IoT projects, the remarkable step was taken by National Agency for Food and Drugs Administration and Control (NAFDAC). Faced with perennial counterfeiting problem, NAFDAC in 2010 resorted to product verification initiative using Radio Frequency Identification (RFID). The technology carried out in collaboration with Verification Technology Limited (VTL), use tags equipped with RFID to secure the genuineness of drugs throughout their supply chain starting from manufacturers, distributors, wholesalers, retailers and even consumers [41].

An economic security application of IoT is the tracking of oil tankers and vessels by the Nigerian National Petroleum Corporation (NNPC). With vehicle tracking and fleet management solutions, the Corporation now has the ability to monitor vessels from the loading port to the discharge port, know their travelling speeds, the exact coordinates, destination and expected time of arrival [35].Another important application of IoT in Nigeria was the use of RFID cards and readers in the general elections. The technology was used to check the authenticity of voters in the elections and greatly improved the credibility of the process by its ability to detect fake and cloned Permanent Voter Cards (PVCs), thus curbing massive thumb printing and the undemocratic and unconstitutional culture of political parties purchasing PVCs from voters with the aim of committing electoral fraud [9].Other deployments include the use of pre-paid meters in the electricity industry. The benefits of the meter include an increase in revenue to the electricity company by reducing the overheads that usually characterise house-to-house recovery of revenues, and by also reducing administration cost required in its deployment. It helps the electricity company to determine the actual energy demand, while giving fair bills, control and reliable electricity to consumers [33].

South Africa has been harnessing the power of IoT for the past 10 years even at a time the most popular mobile phone network in Africa MTN (Mobile Telecommunications Network) deployed the technology using cameras connected to each line. This helps nursing mothers to watch nannies keeping watch over their babies while they are out or at work. It helps reduce crime wave in cosmopolitan areas by installing different sensory based camera in main and suburb areas. South Africa enterprises have seen major investment on IoT and this has led to major increase in more innovation, business efficiency, and lower cost of operation [19].

Kenya has become one of the few African economies growing at a fast pace, and becoming the major business hub for the eastern African region, the government in Kenya developed an economic master print to make Kenya an industrialized middle-income economy where her citizens would enjoy high quality of life in clean and secure environment. A research carried out by a team led by Aisha Bryant tried to set up waste lorries with devices, that tell residents which lorry is free for waste disposal, drivers behaviour with residents and orientation of residents amongst all other features of the application; it was discovered that it improved waste disposal amongst residents thereby making the city clean [15].

In Egypt, **s**cientists comprising of academia, researcher together with software engineers steered a committee that showcased various IoTs application to be used to solve the country major problems (societal and innovations) [16]. A very good example of the application showcased was an IoT embedded software chip into phones and devices mostly used in a house (Fridges, camera and Televisions e.t.c.). It was used to manipulate these respective devices from anywhere in the country, which makes devices at home controllable at every given point depending on the nature of task involved [17].

VI. IOT PRODUCT SAFETY HAZARDS

IoT devices are prone to much vulnerability. The vulnerability of IoT devices and products is capable of actually encouraging attacks against consumers as they can be used to direct attacks on the consumer's network. A number of categories of potential product safety hazards have been identified. The categories include a loss of the product's safety features through malfunction or a change in performance due to software updates, a loss of connection to the internet and a corresponding loss of function, the corruption of data used to support a safety feature [8]. There are also potential physical harms from IoT devices and applications.

An IoT device or application could malfunction, either from a defect that existed when the product was sold, or even by a newly-released update or patch from the manufacturer. The ability to update software after an IoT device or application has left the manufacturing facility creates both opportunities and risks. For example, a device that is found to be defective because of defective software could be rendered non-defective by way of an update pushed out over the internet if the device is connected. At the same time, an otherwise non-defective device could be rendered defective by a software upgrade that is itself defective. If an application malfunctions, it could cause a device to act or react in an unanticipated and potentially unsafe manner. Additionally, an application being hacked could also impact the safety of the device, if such a hack were to, for example, speed up or slow down the appliance causing mechanical failure or overheating [6]. The complexity goes deeper: software modifications can directly affect the functioning of the device or application, or they can indirectly create a malfunction if the device or application necessarily works with other technology and the update disrupts its ability to do so. Such a defect might manifest by inadvertently disabling a safety mechanism or another technology connected to a safety device, or by causing the IoT-connected device or application to operate in a manner contrary to the safe operation of complementary devices, applications, or technology [6].

A risk comes in the form of loss of connectivity, which might prevent the IoT device or application from operating correctly. If the product is dependent on connection to the IoT in order to function safely, this could have potential safety implications if the product is not designed to have a "fail safe" in the event that it loses connectivity. The issue will be more acute where the device itself has a protective function, intended to eliminate or mitigate a risk (e.g. a home security system), such that the mere failure of that protective system to operate properly will itself give rise to a safety risk [39].A fault in a device, such as a product serving as a communications hub for a household (e.g. Amazon's Echo), may result in the loss of access or control to the Internet or other connected devices in the home. Concerns have also been raised about the use of the IoT from a "planned obsolescence" perspective (i.e. companies using the IoT to render older products obsolete or slow so that consumers are forced to buy newer versions). This is not unique to IoT devices, as it has been raised in respect of products such as microwaves and cars in the past, but the IoT would theoretically increase a manufacturer's control over their ability to "end" the life of a product at a particular time. However, the ability to do so could also assist manufacturers in preventing users from continuing to use products that are unsafe and/or pose risks to the consumer. The development of connected devices, supported by other technologies, therefore provides greater opportunities for manufacturers to deal with safety at the end of the product's life, thereby better ensuring safety throughout the full product life cycle [39].

The quality and integrity of the data used to support a safety function can also constitute a hazard. To the extent the safety feature relies on certain data, it is imperative that the data be accurate and uncorrupted or the safety feature may not function. Data quality especially is an emerging problem with the IoT, specifically when the data used by automated decisions comes from third-parties without a reliable reputation, or the data lacks attribution or provenance information [28].For example, barcodes are useful as machine-readable numbers identifying a manufacturer or a product, but the ways in which many third-party applications access meta-data are often unclear and thus the information relayed by a barcode could be incorrect. Just as if data is corrupted, if meta-data are incorrect or misleading, it may cause IoT devices and applications to behave unexpectedly or unsafely.

IoT devices and applications could cause physical harms or injury to consumers or their property.Three situations in which an IoT device could potentially cause damage and/or injury have been identified. First, where the IoT device directly causes the damage, for examples, the locks are opened for thieves, or the pacemaker causes a dangerous arrhythmia in the patient. Second, the IoT device did not directly cause the damage but was used as a pathway to the IoT device that caused the damage. For example, where an Internet connected fish tank at a casino was hacked and then used to steal data from the casino network [24]. There the IoT device was the weak point in the security of the system. The third is where the IoT device is compromised and used to perform denial of service attacks on other IoT devices, which causes damage and/or injury 25].One important area where IoT device could directly cause physical damage or injury is wearable product. The close proximity to the body of wearable products may generate a range of hazards. These include hearing loss from an implanted audio device that malfunctions or plays signals from another source, chemical or thermal burns and skin irritation from leaking or faulty batteries or other reactive materials in the device or application, or even muscle strains from powered exoskeletons moving beyond the natural range of a person’s motion as potential hazards of wearable products [8].Augmented and virtual reality devices may also cause eyestrain, eye trauma, eye-development issues, or motion sickness [51]. In more extreme cases, these devices may even cause epileptic seizures [44].

In addition, IoT-connected devices could distract consumers, or users could rely on information provided by such a device in error, and injure them or third parties as a result [52]. For example, a car equipped with a heads-up display operating an augmented reality application could replace a stop sign with a virtual advertisement and thereby cause an accident. Or a user could injure himself or herself simply by tripping over a real-world object while immersed in an augmented or virtual reality and falling. Consumers could also damage property using IoT connected devices, such as by manipulating sensory devices equipped with augmented or virtual reality without sufficient real-world physical space to accomplish the desired motion [44].

VII. IOT LEGAL CHALLENGES

7.1 Complexity of the IoT Technology

With reference to liability, the difficulty will lie in identifying ‘who’ bears the liability. For example, where a device malfunctions or gives out wrong information that causes damage down the chain of connections, where will liability lie? Would it be the German device manufacturer, Chinese installation engineer, American IoT software developer or Norwegian information aggregators/transmitters, Nigerian Internet Service providers or even the individual owner for not updating software or downloading malware from unsecure sites? The complexity of the technology itself and complexity of the contractual arrangements associated with supply produce significant challenges to product liability or allocation of risks [27].

Most IoT devices are inherently complex, due to their interactions with living things, the physical world, other IoT devices and/or other computing devices and systems. Many IoT devices are hybrids of object, software, hardware and service/s, as functionality often requires associated services to be acquired, such as access to cloud data handling facilities and a website interface. Even more complexity arises when IoT devices’ embedment in larger systems is considered. Many entities can be involved in providing the hardware, software, object and services involved. Systems with nested and/or multiple IoT devices, or multiple IoT devices interacting with conventional computing, such as smart homes, can be very complex, both technically and in terms of associated service contracts.[27]. The complexity of IoT device ecosystems can hamper the allocation of liability for faults. Where a single supplier provides the hardware, software and associated services, liability allocation is relatively simple, limited only by whether the type of harm is legitimately excluded under the contract. But where there are multiple providers, the issue becomes uncertain. Defects in an IoT device ecosystem causing detriment to consumers can arise in several places, including physical faults in the dominant object or embedded computer hardware, bugs in the software, corruption or deletion of data or failure of network connections. And the overall detriment may arise from a combination of defects, as where a network failure corrupts data, causing the IoT device to fail to recognise critical inputs. Even where liability is clear, the mobile nature of IoT devices and the differing locations of provider network actors can make practical enforcement difficult. The complexity of IoT devices’ interconnectivity makes it much harder to establish who is liable under traditional laws and regulations when something goes wrong [32].

7.2 Multiple Actors in the Supply Chain

Any IoT supply chain will have a range of actors who are dependent on the smart hardware device. In terms of the manufacturer of the ‘thing’, most IoT products will be compound, with different manufacturers responsible for different aspects of any “thing of things”, such as a smartphone. Even when there is simply one thing, during the process of manufacturing a lot of different people will be involved, contributing components and facilitating the production process. As with many large companies, a network of resellers, retailers, wholesale distributors, and installers is established. Under product liability law, multiple parties in the chain of commerce could be potentially liable. This may include the manufacturer of the product, the manufacturer of one or more component parts, the party that assembles the product, the wholesaler, the retail store that sold the product to the consumer, and even the installer of the product. Many may attempt to point the finger at the user for improperly using the device and/or the device installer for improper installation [25]. With IoT devices becoming more commonplace, the individual product installer could be targeted frequently. Examples could include the house builder who integrates IoT devices such as thermostats into the house, or the technician who wires the house with IP cameras.

When there is a "product" malfunctioning, it may be difficult to determine the perimeter of the liability of each actor in the IoT supply chain. Software that does not present any defects when commercialised but that creates problems at a later stage, once updated, may raise compliance issues with relevant product safety and liability regulations and standards [38]. The matter may be even more complex in the case where a product that caused harm used an artificial intelligence system. As such a system relies on massive amounts of data, it will be hard for an injured consumer (as well as for the product manufacturer and other actors in the supply chain) to understand why a product took a specific decision at a specific time. In the case, for example, of an accident involving a car using AI/auto pilot mode, the potential liability of the car manufacturer, who may not be in a position to anticipate how the car will behave in the future, is being questioned by stakeholders. More generally, at issue is the ability for consumers and other IoT players to identify the defect that caused damage and the causality between both in an environment where the source of the problem may be linked to, for example, a bug in software or an Internet connection, or to a defect in one or some of the devices used in an IoT ecosystem. Who should bear the burden of proof may in such context prove difficult to determine. Furthermore, the extent to which product liability laws and regulations may apply in an IoT context where a defective "product" may be a mix of hardware, software and services may need to be explored [36].

In applying civil or criminal liability as a result of physical harms the responsible parties need to be identified [58]. However, with the IoT, the causal networks are complex, and determinations of liability can be quite complex. Suppose multiple parties bear a causal relationship to some injury, such that their respective causal contributions have to be partitioned. For example, a driver of a smart vehicle negligently fails to update his firmware, thus leading to a preventable accident with some other motorist who negligently ran a red light. What if the homeowner failed to repair the lock on some expedient timeline? Causal analysis can get complicated.The interdependency of goods and service producers, actors and consumers in the IoT ecosystem means that liability could be difficult to allocate as there are challenges in identifying the root cause of product failuresFor example, in the context of a car accident involving an autonomous vehicle, a number of IoT actors may be wholly, or partially responsible for the accident; these may include the application determining the movement of the car, the manufacturer of the sensors, the operator of the sensor network, the road operator, and the third party that provided the software [30].

7.3 Complexity of Contractual Arrangements

The nature of IoT device ecosystems promotes the likelihood of numerous actors in the provider network. A complex network means complexity in contractual arrangements and therefore liability allocation. Even a basic IoT device such as a thermostat may require many separate contracts dealing with hardware, software development, software licences, installation, website and app usage, payment services, connectivity provision, sale, distribution and rental. These contracts may be with separate entities, some having no connection with (or knowledge of) others in the network. The complexity of contractual arrangements within a network can make it difficult to identify all applicable contracts, let alone interpret them for end-customers (including enterprises) and network actors. Nigerian consumers are particularly affected, as most IoT devices they purchase are imported, with contracts likely to contain foreign jurisdiction and foreign law clauses. Contract drafters for provider networks also inevitably attempt to avoid liability, using favourable jurisdiction and choice of law clauses, or arbitration and class action waivers—practices already common in conventional ecommerce. These impediments, combined with the usually low value of a customer claim relative to legal costs, often hinder customers achieving redress [27].

7.4 Security

Many IoT devices are susceptible to security risk. Consumer devices such as home and appliance monitors, automobile black boxes, personal health monitors, smartphones and employee monitors generate huge amount of valuable data about their users' activities, habits, personalities, preferences and attributes. This goes to expose the grave dangers of these IoT devices despite their flurry of benefits to mankind. As an end-point device, IoT products are less secure than their computer counterparts from both a design and user standpoint. While a hacker cannot access home computer directly, connected devices such as smart TVs, smart light bulbs, security cameras, and thermostats may provide a way for hackers to access a home network to backdoor a network security perimeter and access a connected computer. IoT connectivity gives rise to increased vulnerability, in particular due to cyber security risks (as external attackers might access products remotely in order to cause harm) and privacy risks (as the data collected by connected devices may easily be transferred to third parties) as well as a number of related risks, such as risks of fraud. The U.S. Department of Homeland Security (DHS) asserts there is no clear understanding of who is responsible for security decisions in a situation in which one vendor designs a device, another supplies component software, another organization operates the network in which the device is embedded, and another deploys the device [60]. It argues that this challenge is amplified by lack of comprehensive widely adopted international norms and standards for IoT security, lack of incentives for developers to adequately secure products and unequal awareness of the methodology of evaluating security features of competing options [60].

Privacy and security threats are in the front of IoT's problematic concerns. In the IoT environment, information collected by sensors, chips, smart phones, etc., create vast amount of data and therefore, data volumes expand between 50 and 60 percent every year [47]. These volumes include a very valuable and sensitive data such as personal and financial data. The problem here is that IoT devices are prone to security breach and privacy law is unprepared to curb the threats created by the Internet of Things [48].

7.5 Compensation for Harm/Injury

IoT devices and applications are generally, by the nature of their design, dependent on third party technology to perform their basic functions and maximise benefit to the consumer (Alliance for Internet of Things Innovation [2], and the performance and the safety of a product may be altered by inputs from third parties after the product has been placed on the market. Questions also arise as to the extent to which a supplier of hardware or software should be responsible to ensure the product is protected from a digital security attack on an ongoing basis. This can become particularly challenging in a world in which cyber-criminals are constantly devising new ways to unlawfully access data in order to commit their crimes, forcing those who create the products to continue to develop patches and protections to ensure the ongoing protection of the products in the field.

One conceptual difficulty that remains with each hack is: what damage was actually done and how should victims be compensated? Lucas Amodio contends that where data are compromised by hacks, it is often hard to quantify the damage caused as opposed to physical damages [25]. In many cases, however, it will be difficult to determine the exact fallout of these data breaches. Although it is evident the data are stolen, information on how the data are being used to hurt the victims is not readily available [31]. As a result, courts have had challenges in determining standing and quantifying damages based on data breaches. As a threshold matter, can the plaintiff prove that the harm allegedly suffered was directly caused by the data breach in question? Courts are beginning to require that plaintiffs prove that a specific data breach was the cause of their harm. The second challenge is showing that the plaintiff was actually harmed by the data breach [57]. In a 2017 case from the D.C. Circuit, *Attias v. CareFirst, Inc*.,865 F.3d 620, 625–26 (D.C. Cir. 2017), the court dismissed all of the claims for damages except for two individuals that claimed actual identity theft. As these claims are more nebulous and more directed to the potential for harm than actual, quantifiable harm, litigants will have a more difficult time proving injury in fact.

Although plaintiffs have successfully alleged that they were damaged solely by nature of their data being stolen, such as the Target breach settlement of $18.5 million[21], Yahoo's $117.5 million class-action settlement [20],and the Equifax breach settlement with up to $425 million for those affected by the breach [11], the actual damages are hard to quantify. Despite the increasing amounts of the settlements in these cases, there is no standard for how to calculate damages for individuals whose private information is compromised. For example, in the Equifax settlement, some of the damages include paying those affected $25 an hour for time spent recovering from identity theft or fraud [20].

Damages directly related to physical injuries or property damage is quantifiable and can be addressed, not by data breach theories, but by product liability law. So what happens if an Internet of Things (IoT) shower is hacked and the user is burned, or the shower is caused to constantly run, causing flooding? In most circumstances, the hacker is unavailable, judgment-proof, or may be outside of the jurisdiction [10]. At this point, consumers may turn to product liability law to recover on their losses from one or more of the manufacturers, sellers, retailers, and or IoT device installers.

7.6 Disclaimers of Liability

IoT devices pose significant challenges to the existing product liability framework. Unlike "dumb" devices, IoT products are usually embedded with software that enhances their functionality. In order to use this software however, consumers must first agree to the software's term of services. These licences typically force consumers to assume all responsibility for any damages caused by the product. The Nest thermostat End User Licence Agreement (EULA), for example, states that:

> NOTWITHSTANDING ANYTHING TO THE CONTRARY AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEST LABS PROVIDES THE PRODUCT SOFTWARE "AS-IS" AND DISCLAIMS ALL WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, QUIET ENJOYMENT, ACCURACY, AND NON-INFRINGEMENT OF THIRD-PARTY RIGHTS [34].

When users accept agreement of this nature, they enter into a contract where they effectively relinquish their rights to sue for any damages caused by the device in question, whether for direct damages resulting from dysfunctional device software or for indirect damages resulting from dysfunctional behaviour.

Most IoT devices have restrictive software license agreements that disclaim all liability. Under these agreements, if a malicious user compromise one's Internet connected device or hack one's Internet-connected product, the consumer would have no recourse for compensation. While manufacturers have some need to limit their product liabilities, the breadth and ubiquity of these disclaimers could effectively put an end to product liability as Internet-connected products replace their traditional counterparts. This may hinder consumer protection through product liability law. Manufacturers should exercise caution in drafting their agreements to carefully define liability for product failures. Whilst this can be difficult in a changing legal and regulatory landscape that has not caught up with technology, contract law might evolve to better protect IoT-device users, either through strengthening the unconscionability/ unreasonableness doctrine or by employing public policy arguments to limit the scope of corporate exculpatory clauses.

VIII. Conclusion

Defects in IoT products are difficult to identify as a result of challenges posed by complexity of the technology and multiplicity of actors involved in the manufacturing of the products. IoT technology has physical presence and capacities, some of which might threaten physical safety. It is expected that manufacturers of IoT be significantly concerned with physical safety. IoT safety involves manufacturers being able to reason about the behaviour of IoT devices, especially actuators, and being able to detect and prevent unintended or unexpected behaviour. One of the main product safety-related issues raised by the IoT market concerns ways in which liabilities may be allocated among the various actors of the supply chain in the event technology behaves in an unpredictable and unsafe manner, and causes damage. It is not clear who is responsible for security decisions in a world where one organization designs a device, different entity supplies component software, another operates the network in which the device is embedded, and another deploys the device. Challenges posed by emergence of IoT would cause courts to reconsider the scope of product liability laws and how they should be shaped for the future.

There is the need for policy makers and other stakeholders to join forces and identify the risks that consumers may face in a dynamic IoT marketplace. While stakeholders should bear in mind some of the IoT product safety-related challenges such as liability issues in a complex supply chain, manufacturers should ensure product safety controls and management in an environment where their products, which are interconnected with other manufacturers' products, can increasingly take, anticipate and predict decisions without human intervention. Consumer product safety regulations and standards may in this context effectively address the resulting product safety issues and consumer damages. This will involve reviewing the adequacy of key product safety concepts and definitions, such as "product", "safety", "damage" and "liability," in today's environment where products can become defective and unsafe as a result of incidents, such as a data breach. Initiatives should also be driven by legislation to enact relevant laws to address challenges associated with the IoT or find ways to expand the existing laws.Consumers should be aware of all facts about IoT devices and processes, especially the way they generate, collect, store or share information. This is believed to be the first step which will enable lawmakers to examine the risks or hazards associated with the IoT and then take necessary policy and legislative actions.

With the aid of relevant science and technology authorities, stakeholders should be prepared to establish standards that are tailored specifically to IoT product safety and other related matters. IoT developers should factor in security, user experience, resiliency and adaptability when a device, sensor, service or any IoT component is being designed and developed. Many of the vulnerabilities of IoT products could be mitigated through recognized security best practices and self-regulatory efforts. Government oversight and enforcement of minimum safety standards is important considering the possibilities of physical risk IoT and applications could cause.

REFERENCES

[1]. African Review of Business and Technology, South Africa one of the fastest-growing IoT markets in the MEA region, Alain Charles Publishing Ltd. 2021 https://www.africanreview.com/finance/business/south-africa-one-of-the-fastest-growing-iot-markets-in-the-mea-region

[2]. Alliance for Internet of Things Innovation, Working group for report on policy issues. (2015), Https://Aioti-Space.Org/Wp-Content/Uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf.

[3]. Andy, G., Hackers Remotely Kill a Jeep on the Highway—With Me in It. 2015 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[4]. Bao K., et al., Liability for Home IoT 2015 http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall15-papers/Liability%20for%20hone%20IoT.pdf

[5]. Bill, W., In the Programmable World, All Our Objects Will Act as One. 2013), https://www.wired.com/2013/05/internet-of-things-2 [https://perma.cc/UG4T-RXV7].

[6]. CertifiGroup, International Regulatory Compliance. 2016 http://certifigroup.com/whitepapers/product-safety-and-iot.pdf

[7]. Cisco, The Internet of Things how the next evolution of the Internet is changing everything

[8]. Consumer Product Safety Commission (CPSC) (US) Potential hazards associated with emerging and future technologies. 2017, https://www.cpsc.gov/s3fspublic/Report%20on%20Emerging%20Consumer%20Products%20and%20Technologies_FINAL.pdf

[9]. Ekujumion, N., Still on card readers for 2015 election. 2015 http://thenationonlineng.net/still-on-card-readers-for-2015- elections/

[10]. Eldar H., The cyber civil war, 44 Hofstra Law Review. 2015 41.

[11]. Equifax Data Breach Settlement, Federal Trade Commission.2020) https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

[12]. Federal Trade Commission (US), Internet of Things, privacy and security in a connected world, FTC Staff Report, January 2015, www.ftc.gov/system/files/documents/reports/federal-tradecommission-staff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127iotrpt.pdf.

[13]. Goldberg, J., et al., The easy case for products liability law: A response to Professors Polinksy and Shavell. Harvard Law Review, 2010. 123(8): 1919–48.

[14]. Gubbi, J., et al., An information framework for creating a smart city through the internet of things. IEEE Internet of Things Journal, 2014. 1(2): p. 112–121.

[15]. http://ibmresearchnews.blogspot.com/

[16]. http://iot-egypt.com/steering-committee/

[17]. http://siapsprogram.org/tools-and-guidance/edt/

[18]. John A. R. Net Gets Physical: What you need to know about the Internet of Things, 2014, https://www.americanbar.org/groups/business_law/publications/blt/2014/11/03_rothchild/.

[19]. Kalebaila, G., Internet of Things in Africa 2016, https://www.idc.com/getdoc.jsp?containerId=CEMA43088517.

[20]. Kelly T., Yahoo data breach settlement 2019: how to get up to $358 or free credit monitoring, USA Today. 2019 https://www.usatoday.com/story/money/2019/10/14/yahoo-data-breach-117-5-million-settlementget-cash-monitoring/3976582002/.

[21]. Kevin M., Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers, USA Today. 2017 https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach- affectedconsumers/102063932/.

[22]. Kim, Z., Hacker lexicon: What are white hat, gray hat, and black hat hackers? 2016 https://www.wired. com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/.

[23]. Kranenburg, R. The Internet of Things, draft paper prepared for the1st Berlin Symposium on Internet and Society. 2011.

[24]. Lee M., Criminals hacked a fish tank to steal data from a casino, Forbes. 2017 https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-tosteal-data-from-a-casino/#5feb50d332b9.

[25]. Lucas, A., Is the Internet of Things Ripe for Product Liability Law? Linkedin. 2016, https://www.linkedin.com/pulse/internet-things-ripe-product-liability-law-lucas-amodio-c-eh/.

[26]. Lucas, A., The intersection of product liability law and the Internet of Things. Boston College Intellectual Property and Technology Forum, 2021.

[27]. Manwaring, K. and C. Hall. Legal, social and human rights challenges of the Internet of Things in Australia. Input paper for the Horizon Scanning Project "The Internet of Things" on behalf of the Australian Council of Learned Academies. 2019. https://acola.org/wp-content/uploads/2021/02/acola-iot-input-paper_legal-social-and-human-rights-challenges_manwaring-hall.pdf

[28]. McAfee (2013), Data quality in the Internet of Things, https://securingtomorrow.mcafee.com/business/data-quality-in-the-internet-of-things/

[29]. Mckinsey Global Institute, The Internet of Things: Mapping the value beyond the hype 2, 7 (2015), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[30]. Medium, IoT Raises new challenges for assigning liability. 2017, https://medium.com/iotforall/iot-raises-new-challenges-for-assigning-liability-7387b65decd0.

[31]. Michael H., et al., Have we reached the tipping point? Emerging causation issues in data-breach litigation, FLA Bar Journal. 94 (8): 2020 p. 9–16.

[32]. Michael, K., IoT and liability: Who pays when things go wrong? Techrepublic. 2016 https://www.techrepublic.com/article /iot-and-liability-who-pays-when-things-go-wrong/.

[33]. Naijatechguide, PHCN: Benefits of the new prepayment meters. http://www.naijatechguide.com/2007/11/phcn-benefits-of-new-prepayment-meters.html.

[34]. Nest, End User License Agreement. https://nest.com/ae/legal/eula/.

[35]. Nigerian National Petroleum Corporation, NNPC acquires state of the art tracking device to keep tab on in-coming oil vessels. 2015 http://www.nnpcgroup.com/PublicRelations/NNPCinthenews/tabid/92/articleType/ArticleView/articleId/80/NNPC-Acquires-State-of-the-Art-Tracking-Device-to-keep-tab-on-In-Coming-oil-Vessels.aspx

[36]. OECD, Protecting and empowering consumers in the purchase of digital content products, OECD Digital Economy Papers, No. 219, OECD publishing, paris,2013.

[37]. OECD, The Internet of Things: Seizing the benefits and addressing the challenges (2016). OECD Digital Economy Papers, No. 252, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwvzz8td0n-en.

[38]. OECD, Consumer product safety in an era of technology-driven products and supply chains: Project proposal. working party on consumer product safety, Paris 2017.

[39]. OECD, Consumer product safety in the Internet of Things, OECD Digital Economy Papers, OECD Publishing, March 2018 No. 267.

[40]. Ofcom, The Communications Market 2018. https://www.ofcom.org.uk/research-and-data/multi-sector-research/cmr/cmr-2018/interactive

[41]. Onyalo, N., et al., The Internet of Things, progress report for Africa: A survey. International Journal of Computer Science and Software Engineering, 2015. 4(9): p. 230-237.

[42]. International Telecoms Union, Overview of the Internet of Things recommendation ITU-T Y.2060, ITU 2012 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559.

[43]. Public Service Announcement: Motor Vehicles Increasingly Vulnerable to Remote Exploits, Fed. Bureau

[44]. Reed, S., Augmented and virtual reality: emerging legal implications of the "final platform. 2017,

[45]. ReportLinker, Internet of Things (IoT) market - growth, trends, COVID-19 impact, and forecasts (2021 - 2026) 2021 https://www.reportlinker.com/p06067771/Internet-of-Things-IoT-Market-Growth-Trends-COVID-19-Impact-and-Forecasts.html

[46]. Sam, L., IHS Tech., IoT Platforms: Enabling the Internet of Things 5 (2016), https://cdn.ihs.com/www/pdf/enabling-IOT.pdf,

[47]. Samuel, G., The Internet of Things. Massachusetts Institute of Technology, 2015.

[48]. Scott, R. P., Regulation of the Internet of Things: First steps toward managing discrimination, privacy, security, and consent. Texas Law Review, 2014 9(1), p 85.

[49]. Sonar Trend Platform, the Evolution of Consumer IoT

[50]. Sonny, Z., The concept of Internet of Things and its challenges to privacy. South East Asia Journal of Contemporary Business, Economics and Law, 2015. 8 (4): p 1-6.

[51]. Street, R., Reality check: The regulatory landscape for virtual and augmented reality", R Street Policy Study, 2016. 9(69): https://www.rstreet.org/wp-content/uploads/2016/09/69.pdf

[52]. Tech Policy Lab, Augmented reality: A technology and policy primer. 2015 University of Washington, http://techpolicylab.org/wp-content/uploads/2016/02/Augmented_Reality_Primer-TechPolicyLab.pdf

[53]. TechUK, The State of the connected home. 2018 https://www.techuk.org/resource/the-state-of-the-connected-home-campaign-week.html

[54]. Telefonica, 5 Amazing Things made reality by IoT technology. 2016, https://iot.telefonica.com/blog/5-amazing-things-made-reality-by-iot-technology-toys-edition

[55]. The World Population Prospects: 2015 Revision, United Nations Dep't Econ. & Soc. Aff., July 29, 2015, http://www.un.org/en/development/desa/publications/world-population-prospects-2015-revision.html.

[56]. Thierer, A., The Internet of Things and wearable technology: Unlocking the next wave of data driven innovation, Presentation at AEI-FCC Conference on Regulating the Evolving Broadband Ecosystem, Mercatus Centre of George Mason University, 11 September 2014, www.aei.org/wpcontent/uploads/2015/03/thierer-final-internet-of-things-presentation_104713970943.pdf.

[57]. Thomas R. and E. Goodman. Yes, but were you hurt? Another data breach case dismissed for lack of damages, 2019 https://www.classactiondeclassified.com/2019/08/yes-but-were-you-hurt-another-data-breachcase-dismissed-for-lack-of-damages/#page=1.

[58]. Twerski , A. et al., Product liability: A study of the interaction of law and technology. Duqesene Law Rev.1974. 12(3): p. 425–464.

[59]. U.S. Consumer Product Safety Commission. Statement of Commissioner Elliot Kaye regarding a framework of safety for the Internet of Things, 2019.

[60]. U.S. Department of Homeland Security (DHS). Strategic principles for securing the internet of things (IoT).Version1.0. (2016) https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINALpdf

[61]. Wood, A. The internet of things is revolutionizing our lives, but standards are a must. The Guardian Newspaper, March 31, 2015.