UNITED NATIONS
CENTRE FOR TRADE FACILITATION AND ELECTRONIC BUSINESS
(UN/CEFACT)

REGULATORY AND EGOVERNMENT PROGRAMME DEVELOPMENT AREA
EDATA MANAGEMENT DOMAIN

INTERNET OF THINGS PROJECT

IoT in Trade Facilitation Whitepaper

SOURCE: IoT-TF Project Team
ACTION: Public Review

DATE: **12 October 2021**
STATUS: **Draft for Public Review**

Draft Document

UN/CEFACT

IoT in Trade Facilitation

Whitepaper

Version of 11-October-2021

UN/CEFACT Whitepaper on IoT in Trade Facilitation

Contents

1. Introduction

The Internet of Things (IoT) is no longer a term used exclusively by technical experts. The Internet of Things (IoT) is becoming an integral part of business and supply chain management, providing data that supports inventory management, equipment maintenance, building management, insurance claims and the tracking and tracing of a wide variety of assets. Therefore, it has also become an essential tool in trade.

The Internet of Things helps people and businesses to be and act smarter. The increasing use and utility of IoT ecosystems is reflected in worldwide annual spending on IoT which reached over $742 billion in 2020 and is expected to reach over 1 trillion dollars by 2023[1]. The vast majority of that expenditure is by businesses, looking to improve operational efficiency and find new revenue opportunities.

Trade facilitation is "the simplification, standardization and harmonization of procedures and associated information flows required to move goods from seller to buyer and to make payment"[2]. IoT ecosystems can support trade facilitation by providing data that be used for simplified procedures. For example, status and location data can be used to reduce the need for inspections and manual verification, it can also be used to support certificates of origin (or might even replace them some day). IoT location and environmental data can be used to simplify insurance claims for everything ranging from late delivery to goods damaged by the environment (temperature, humidity, excess motion, etc.) and they can also be used to support reconciliation in goods accounting (for example, reconciliation between purchase orders and deliveries), including for letter of credit payments.

At the same time, for IoT to fully support trade facilitation, standardization of IoT data is needed. Trade facilitation, by its very nature, requires the exchange of data between different parties. Thus, the usefulness of IoT data for facilitation is dramatically reduced if everyone uses different definitions and formats for their data as this results in a burdensome network of data translation needs that multiply exponentially with the number of participants. UN/CEFACT can provide solutions to this problem through its Core Components

[1] https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/ (accessed on 26-01-2021). See also, International Data Corporation (IDC) Worldwide Semiannual Internet of Things Spending Guide of June 2020 at https://www.idc.com/getdoc.jsp?containerId=prUS46609320# (accessed on 07-10-2020)

[2] Trade facilitation implementation guide, available at https://tfig.unece.org/details.html (accessed on 14-08-2021)

Library (CCL), which provides data definitions and code lists. The challenge remains, however, to make the existence of the CCL known to IoT system developers, with easy-to-access information about its use, and to ensure that the data which is needed can be found in the CCL. The UN/CEFACT smart container project has made important steps toward ensuring that the required data is available, but more work is needed to ensure that IoT data used in other areas, such as inventory management, accounting, and finance, are fully reflected.

For a more in-depth discussion of standards and the potential need for new standards to support the use of IoT in trade facilitation please refer to the UN/CEFACT Whitepaper on IoT Standards for Trade Facilitation[3]

The objective of this paper is to help readers better understand both IoT and how it can be used to support trade facilitation and government infrastructure management. It is organized in three sections:

- Section 1 seeks to provide an overview of the technologies used in IoT for trade-related applications. The objective has been to provide explanations that are accessible to those who are familiar, as managers, with information technology, but perhaps have little or no experience with IoT.
- Section 2 looks at how the IoT can be used to support trade, supply chains and government infrastructure management.
- Section 3 looks at the legal challenges when implementing IoT in support of trade.

Section I Overview of IoT Technologies

What is the Internet of Things? The following is one definition found in the IEEE Internet of Things Journal.

"An IoT system is a network of networks where, typically, a massive number of objects, things, sensors or devices are connected through communications and information infrastructure to provide value-added services via intelligent data processing and management for different applications (e.g. smart cities, smart health, smart grid, smart home, smart transportation, and smart shopping)."

[3] Insert relevant future reference

In order to part of the Internet of things (IoT), the above mentioned "objects" or "things" (hereafter referred to as "devices") must have unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.[4]

IoT devices may:

- Include one or more sensors (for temperature, humidity, movement, etc.)
- Transmit the device's location (using calculations or GPS)
- Both transmit information and receive instructions. For example, if you send a signal to your home from work in order to adjust the thermostat or start the oven.
- Include some processing intelligence, for example analysing and only transmitting sensor data when it is outside a prescribed range
- Collect data from other IoT devices for transmission or initial analysis, if they analyse data they are called **edge-computing devices**
- Be embedded in a living entity such as an animal or human being. For example, a heart monitor that periodically transmits information to a system which can send alerts to the human wearing the device or their doctor.

What kinds of data are collected by IoT devices?

- Status data – This is the most basic type of IoT data and is primarily used as raw material for more complex analyses - but can also have a significant value of its own. A common trade example is sensors in shipping containers that indicate their internal temperature or humidity.
- Location data – Is data that identifies the location or position of an object of interest. International trade has many examples of IoT for tracing trucks, containers and products.
- Automation data – This is sensor data that supports the control of processes and carries out functions like monitoring and adjusting heating systems, lighting, warehouse conditions, etc.
- Actionable data – This is IoT data that, when analysed, results in proposals for action to optimise solutions such as recommendations for cutting excess energy consumption in buildings or informing managers of the need for preventative maintenance of equipment (for example, trucks or forklifts).
- Feedback data – IoT can also create a feedback loop from the end consumer to the manufacturer, allowing product developers to examine real-world behaviours – while preserving appropriate levels of privacy, security, and anonymity

[4] Modified from https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

The data captured or generated by an IoT ecosystem may be transmitted directly to an application (on the cloud or a blockchain or a private server) or it may be fully or partially analysed locally before being transmitted. When IoT ecosystems generate large volumes of IoT data, the applications that use this data are often located in the cloud and/or may use artificial intelligence to analyse the data.

IoT applications often deploy devices in networks (**ecosystems**). For example, a warehouse building may have an IoT ecosystem that monitors a range of building conditions and controls equipment in order to maintain a certain temperature and humidity range at a minimum cost and alert management to any problems.

The Internet of Things helps people and businesses to be and act smarter. It can provide real-time insight into a broad range of conditions and activities. Just a few examples are:

- The location of shipping containers
- Environmental conditions inside of containers or buildings such as factories
- Traffic conditions in a city
- The availability of parking or storage space
- The performance of manufacturing equipment
- A patient's blood pressure
- The irrigation of crops

2. IoT Devices and Technology

In order to be effective, IoT devices have a wide range of requirements, some related to the devices themselves and some to the IoT ecosystems in which they operate. A summary of the main requirements indicates that an IoT device should:

- Include **sensors, transmitters** and/or **receivers**,
- Be **small, low power (with long battery life) and low cost**.
- Have a **unique identity** and an **identifiable location**
- **Transmit data** either over short-range distances, to other IoT devices, or over medium- to long-range distances
- **Communicate** and **share data** with other systems (which requires **interoperability)**
- **Be maintained** both in their hardware and software
- **Be secure** and protected from unauthorized access and data falsification
- Operate **in a legally correct way**

There are new technologies being discovered every week, if not every day, that can impact these different IoT requirements. In this section, a modest attempt is made to look in more detail at the above issues and related technologies with the exception of legal issues which are looked at in Section III.

2.1 Kinds of IoT Devices

There are many different types of IoT devices, the broad categories looked at here are: those with sensors, those without sensors, edge-computing devices and IoT gateways.

2.1.1 IoT devices with one or more sensors or actuators

Sensing technologies combined with IoT devices provide the means for creating information that reflects an awareness of the physical world. IoT sensors collect information which is processed at one or more layers in an IoT ecosystem. For example, the collecting IoT device may decide if a temperature reading is within range, or it may transmit it to a nearby IoT edge-computing device for this decision. Then, only "out of range" temperature readings are communicated to a further computing layer for additional analysis and processing. The growing number and kind of sensors which can be included in small IoT devices is made possible by developments in nanotechnology and, more specifically, in micro-electromechanical systems (MEMs). These are miniature machines with electronic and mechanical components such as springs, channels, cavities, holes, and membranes. They range in size from several millimetres to less than one micrometre (i.e. much smaller than the width of a human hair).

From an IoT standpoint, the most interesting MEMs are sensors (to detect a state) or actuators (to control a process). Microsensors exist for a multitude of tasks including the sensing of temperature, pressure, humidity, motion, chemicals/gases, magnetic fields, radiation, etc. Existing types of micro actuators include: microvalves and pumps for control of gas and liquid flows; optical switches and mirrors to redirect or modulate light beams, micro flaps to modulate airstreams on aerofoils and many others.

Progress in MEMS depends on developments in microfabrication techniques (including for their incorporation into integrated circuits) as well as on clever design. MEMS are also referred to as micromachines, micromachined devices or microsystems technology (MST).[5]

[5] Resource 1) https://internetofthingsagenda.techtarget.com/definition/micro-electromechanical-systems-MEMS and Resource 2) https://www.mems-exchange.org/MEMS/what-is.html (both accessed on 25-08-2020)

2.1.2 IoT devices without sensors

Some IoT devices do not include sensors and, instead, only receive and transmit information. For example, an IoT device may receive instructions from a distance to unlock or lock a door, start a machine, etc. - or an IoT device may collect information from other devices, for example, sales or activity data from multiple cash registers in a store.

2.1.3 Edge-computing devices

Edge-computing IoT devices collect data from other IoT devices and provide a range of benefits which are described below and include several which reduce overall IoT system costs.

- **Reduced device costs** by moving more expensive analytic computing tasks computation tasks away from individual IoT devices and allowing connected devices to be equipped with only short-range transmission capabilities.
- **Reduced data transmission costs**, by analysing IoT data and only transmitting data which meet defined criteria
- **Lower latency**: Because computation is performed closer to data origin, there is less transfer time. This is beneficial in manufacturing process and medical applications where real-time feedback and quick responses are essential.
- **Data privacy**: Edge computing creates more options for data treatment. For example, it has the potential to solve some personal data protection issues by processing personal data locally and only transmitting forward anonymous results for further processing or storage.
- **Higher security**: Centralized architectures are vulnerable to distributed denial of service (DDoS) attacks. A decentralized edge-computing architecture makes it difficult for a single disruption to take down the entire system.
- **Scalability**: Edge-computing architecture can offer a more flexible expansion of computing resources as more devices are added to an IoT system by reducing the computing, transmission and storage burden on a central system. As one example, an edge-computing device could analyse the results from many sensors on a second-by-second basis and only forward 1) averages over set periods of time and/or readings that are outside of a prescribed "normal" range.
- **Reduced maintenance costs and environmental impact**: by deploying simple IoT sensors in the field, and pushing computing functions to the IoT Edge, the field deployed IoT devices require less

computing power which increases battery life. This results in less frequent servicing and, by extending battery life, reduces waste.

2.1.4 IoT gateway devices

An IoT “edge-computing” device which is dedicated to data transmission is called an IoT gateway device. These are used to reduce the cost of telecommunications by receiving long distance communications and then distributing them onwards to less expensive IoT devices with lower power needs and shorter-distance communications capabilities (e.g. Bluetooth) as well as collecting data from these IoT devices and then transmitting them onward over longer distances.

2.1.5 IoT Energy Requirements

One of the key operational challenges when implementing an IoT network is power consumption. Many IoT components (especially when used in transport) need to be relatively simple and able to operate for long periods of time, unattended and in remote locations. This highlights the need for low power consumption, long battery life and strategies for maintaining signal (communications) integrity.

These requirements result in a number of design considerations which depend upon the IoT application, and the communication channel being used for data transmission. For instance, the best way to conserve power for an IoT device with a wireless radio is to ensure that the radio is only fully powered when in use. Similarly, in the case of cellular channels, it is important to choose an efficient and secure communication protocol that requires minimum overhead. In the case of Bluetooth, low energy transmitters are available which allow devices to be in sleep mode and only become active when an event occurs.

Despite the availability of technologies that enable low power consumption, large IoT deployments involving thousands of devices can still present serious energy-related maintenance challenges. For example, the need to detect and change devices that fail and the possibility that many batteries (or devices if the batteries are so integrated that they cannot be changed) may need to be replaced at their end of life and during a similar period. For example, if 10,000 devices with a 3-year battery life are put into commission over a 2-year period there will be 5000 batteries or devices to be changed in the 4th and 5th years.

2.1.6 Location – for Devices and Target Objects

The location identification needs for a device are determined by the IoT application/ecosystem. If an IoT device is relatively immobile (such as a sensor in a traffic light) then it may need to transmit its location only upon installation or being moved (or its location may be registered by the installer, thus removing the need for transmission). On the other hand, if the IoT device is attached to an asset that is being tracked such as a package or a shipping container it may need to transmit its location several times, or more, a day. Most IoT devices are low-power – and the more power needed for determining and transmitting location – the more expensive the IoT device and the more often it needs maintenance.

If only the approximate location of the IoT device is needed (e.g., if stock has passed through a loading dock or is in an identified building or site) then having an IoT gateway device simply detect the presence of simpler, more passive IoT devices (such as RFID tags) may provide sufficient location information.

More precise location information is determined using radio-signal transmitters and receivers. The shorter the range of radio-signal transmitters and receivers, the less power they need. This makes GPS one of the most expensive solutions. One way the cost of GPS can be minimized is by using a more powerful edge-computing device to: i) collect IDs from devices within a low-energy transmission distance (and, if needed calculate their exact position), ii) receive the GPS signal, calculate the position and iii) transmit the position with the collected IDs (perhaps via satellite). Such edge-computing devices can be installed on transportation vehicles such as trucks or ships to collect location information about the packages and/or containers that they carry.

The principal methods for determining location with radio-signals are:

- GPS: A radio-signal receiver receives a radio signal transmitted by a GPS satellite which it uses to calculate its position.
- The use of registered signalling devices to determine (via an online database[6]) or calculate (based on a method called “triangulation” or “trilateration”[7]) the location of the radio-signal receiver in an IoT

[6] This is a Media Access Control (MAC) address (for Wi-Fi), a Bluetooth© Low Energy (BLE address) or information obtained from a Cellular base station’s combined Cell ID (CID), Location Area Code (LAC), Mobile Country Code (MCC), and Mobile Network Code (MNC) https://cellidfinder.com/articles/how-to-find-cellid-location-with-mcc-mnc-lac-i-cellid-cid. MAC and BLE formats and IDs are determined by IEEE (https://www.ieee.org/) and for cellular base stations (CID, LAC, MCC and MNC) the standard is maintained by 3GPPP (https://www.3gpp.org/)

[7] For MAC https://whatismyipaddress.com/mac-address and for BLE https://reelyactive.github.io/ble-identifier-reference.html and for Cellular base stations https://combain.com/about/about-positioning/cell-id-positioning/ and for trilateration techniques: Ana Roxin, Jaafar Gaber, Maxime Wack, Ahmed Nait Sidi Moh. Survey of Wireless Geolocation Techniques. 50th IEEE Globecom07, Nov 2007, Washington DC, United States. ffhal-00701118f - https://hal.archives-ouvertes.fr/hal-00701118/document

device. The exact steps to be taken will vary depending upon whether the registered signalling is from a Wi-Fi access point, a Bluetooth access point or a cellular-base station.

Transmitting the position of other, target objects.

Once the location of an IoT device has been determined, it may need to transmit the position of other, "target" objects (for example, pallets inside of a warehouse). If the IoT device is attached to the target object, such as a container, this is relatively easy – but attaching an IoT device to every target object can be expensive, relative to the cost of the object, and, in some cases, may not be physically possible.

In those cases, there are two principal ways to associate target objects with an IoT device.

i. The radio signal receiver in the IoT device reads individual identification information attached to the target objects such as Radio Frequency ID (RFID)[8] or Near Field Communication (NFC)[9] tags.
ii. Individual identification features of an object are obtained via image analysis (which requires that either the IoT device or a connected edge-computing device have more expensive computing capabilities)

3. Communications and Connectivity

In IoT, it is essential to have data transfer between the IoT layers that acquire physical information, such as location, temperature, chemical composition, etc. and cyber layers that aggregate physical information and perform various calculations and analytical processes. At the same time, data transmission capabilities add costs, both to the IoT device and for the communication itself. In addition, the efficiency, effectiveness, and security of data transmission can be affected by technology choices as discussed below.

3.1 Communications

3.1.1 Communications – Wireless Technology

Most of the communication methods used between devices in an IoT system are based on wireless communication. The two types of wireless communication methods most frequently used are:

- **2.4 GHz band**: which is for short/medium-range transmission and is easy to implement for smartphones and IoT gateway devices. Examples include Wi-Fi, Bluetooth, Zigbee, etc. It is the most

[8] https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm (accessed on 07-10-2020)

[9] NFC tags can only be read from a distance of 4 cm - about 1.5 – inches, or less but are highly secure. For more information see https://nfc-forum.org/what-is-nfc/about-the-technology/ (accessed on 07-10-2020)

convenient communication method because a radio station license is not required in many countries.

- **920 MHz band**: which allows for medium to long range transmission. Examples include EnOcean, Z-Wave, Wi-SUN and Low-Power Wide Area, LPWA, networks (i.e. LoRaWAN, Sigfox, NB-IoT), etc. A radio station license is not required in many countries, but there are countries that have operational rules that set bandwidth restrictions so that a large number of devices can efficiently use the bandwidth.

3.1.2 Communications – formats/standards (i.e. protocols)

Of the wireless communication methods used within IoT systems, the only method included in the Internet protocol suite is Wi-Fi. For this reason, IoT gateways, which collect information from nearby IoT devices, often need to convert the data received into a format that belongs to the Internet protocol suite so that it can be transmitted via the Internet.
The primary Internet protocols used in IoT are HTTP and MQTT, followed by UDP.

- **HTTP**: Originally a communication protocol used for sending and receiving content, such as HTML. It is very simple and versatile, so it is often used in IoT. However, it requires that a message header be attached to both requests and responses, so it tends to be avoided when there are large volumes of data and a need to prevent transmission costs from increasing.
- **MQTT**: A data delivery protocol that allows messages to be kept lightweight, and also includes a specification, called QoS, where a guarantee of delivery level can be specified.
- **UDP**: The lightest weight protocol, however it does not guarantee reliability, order, or data integrity, so it is used only for data transfer (i.e. not for the transmission of instructions/code) and only when delivery confirmation is not needed.

In addition to creating transmission compatibility with Internet protocols, IoT gateways can also provide encryption in order to protect the data within the networks and during data transmission. In this context, gateways can be thought of as an extra layer between the cloud and IoT devices which can filter out attacks and illegal network access attempts.

3.2 Connectivity

3.2.1 Connectivity - Network Technologies

A virtual network is made up of hardware and software which are not physically connected but communicate together according to set a set of standards/rules, usually over the Internet. Characteristics that are important design considerations when developing a virtual IoT network (ecosystem) include signalling, presence detection, bandwidth, communication channel and security.

With increasing demand to achieve lower latency (times between transmission and reception) and higher security, virtual network standards are starting to play a huge role in IoT systems.

For example, **SD-WANs (Software Defined Wide Area Networks)**[10] are often utilized in the telecommunication sector to offer higher bandwidths with faster throughput and the ability to offer lower cost services. In addition, even faster virtual network technologies such as those which utilize mesh networks, are starting to surface. **Mesh Networks**[11] allow any individual node to communicate directly, using Peer to Peer (P2P) encrypted communications, with every other node, or individual nodes, on the same network segment in a fast and reliable manner that resembles that of a LAN (Local Area Network) but over nearly any distance.

Another important network technology, often used in IoT, is **Low-Power Wide-Area Networks (LPWANs)**[12]**.** Many IoT applications need to transmit data over long distances and for long periods of time running to years. Examples are agricultural sensors, warehouse sensors and urban sensors for garbage collection, lighting, parking, etc. The trade-off is that transmissions on LPWAN networks can fail to complete due to interference – so it cannot be used for "mission-critical" applications such as in healthcare or industrial processes -- but if information from an irrigation sensor or a garbage bin are a little late, no harm is done.

Each IoT connectivity option has its own benefits and trade-offs related to data transmission (e.g., amount of data and frequency), latency, power consumption, cost, and security, to name a few. High-volume, fast data transfers generally use more power. Looking for low power consumption? The trade-offs are generally shorter range and less bandwidth.

[10] https://www.networkworld.com/article/3031279/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html (accessed on 2020-10-11)

[11] https://computer.howstuffworks.com/how-wireless-mesh-networks-work.htm (accessed on 2020-10-11)

[12] https://www.iotforall.com/what-is-lpwan-lorawan (accessed on 2020-10-12)

The best option will depend upon the application. Does your organization collect water meter readings across a city? Maybe LoRa (Long Range Wide Area)[13] which is a good option for sending small amounts of data at regular intervals. In an industrial setting that needs to connect millions of small, real-time sensors or requires ultra-reliable, low-latency connectivity? 5G may be best. For agriculture businesses that want to capitalize on IoT, cellular isn't an option -- low-power, long-range WAN may be the best bet.

3.2.2 Connectivity - Data Flows

The core of any IoT ecosystem is the orchestration of data flows. In other words, the routing and interactions between “data packages” coming to and going from: IoT devices including edge-computing and gateway devices, the cloud, other databases/blockchains and operations and/or analytical software applications (including AI systems). In establishing this orchestration, the following should be considered:

- **Interoperability**, in the context of IoT this refers to the ability of systems or components of systems to communicate with each other, regardless of their manufacturer or technical specifications. Why is interoperability needed? Imagine in an IoT ecosystem in an office building where the system that regulates the air conditioning unit “speaks” a different language from the one “spoken” by the system that controls the windows blinds (as programmed by their manufacturers). In that case, these two systems would not be able to communicate with each other and take action in a coordinated manner – resulting in the owner having higher than necessary electrical bills. Given that the technology ecosystem is still in a nascent stage and the market for IoT devices is fragmented, interoperability is a key issue.
    - One example of a standard addressing interoperability issues is IEEE P2413[14] which describes an **architecture framework** for the Internet of Things (IoT). The architecture framework description is focused upon concerns shared by IoT system stakeholders across multiple domains (transportation, healthcare, smart grid, etc.)[15] such as security requirements for IoT communications.
    - Another example is the United Nations Core Component Library[16] standard which supports **semantic interoperability** through standardized data definitions. This interoperability layer

[13] LoRa (short for long range) is a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology - https://www.semtech.com/lora/what-is-lora (accessed on 2020-08-10)

[14] IEEE P2413 - Standard for an Architectural Framework for the Internet of Things (IoT)

[15] https://standards.ieee.org/content/ieee-standards/en/standard/2413-2019.html

[16] https://unece.org/fileadmin/DAM/cefact/GuidanceMaterials/ExecutiveGuides/CCL-CCTS-ExecGuide_Eng.pdf (accessed 2021-01-31)

ensures that data from different systems use the same definitions, for example, for temperature or time as well as for more abstract concepts such as “out of range” (if the range is 4-6, is 6.01 out of range? or only 7?).

    - Interoperability at the level of **data formats** often requires conversions between the standards and communication formats used on an IoT local network and those used on the Internet. In most cases, this process is performed on gateway devices, but it may also need to be incorporated in Application Programming Interfaces (APIs are used for communicating instructions and data between software programmes).
- **The aggregation of data** with defined characteristics from various locations in order to identify trends. Data aggregation may take place in either a local gateway device or a cloud-based central data centre.
- Transferring data to **various data storage locations and media**
- **Eventual changes** to data flows – IoT ecosystems need be designed flexibly so that data flows can be modified at any point order to take advantage of new technologies, new applications and changes in service providers.
- **Generation of learning data for Artificial Intelligence (AI)**: IoT can continuously generate data for use by AI systems for learning and developing inference models. These AI processes can take place continuously or in batches at set times (i.e. once a day, week, etc). This is usually done at a cloud layer because edge-computing devices typically do not have the needed processing power. For more – see the chapter on Artificial Intelligence.
- **Communicating data to blockchains** (distributed ledgers) for use in the automatic execution of smart contracts – for more see the chapter on Blockchain technology.

4. IoT Management and Security

Security in IoT ecosystems looks to protect against external attacks that could compromise or bring down the ecosystem as well as protecting the confidentiality and integrity of data. Some of the more important risks for IoT ecosystems include:

- Man-in-the-middle attacks where hackers intercept and steal or change data as it is transmitted over open networks.
- Botnet attacks where a hacker takes control of a number of devices by exploiting security vulnerabilities within those devices in order to use their computing resources
- Ransomware or other malware which, if installed on IoT devices, can jeopardize an entire IoT ecosystem.

A cyber security framework to address these threats should include a well-defined naming and registration process for devices, a strong system for the authentication of devices, protocols for devices to securely communicate within the network and a platform for managing devices throughout their lifecycle including the ability to shut down or isolate a device if it goes “rogue”. One secure framework is the Zero Trust Design philosophy – which only allows components within an IoT architecture to communicate when they have been specifically granted the right to do so, therefore drastically limiting the ability of components to impact other services should they become compromised.

Device management is also a key challenge both from a security and an operational standpoint. Unlike conventional IT systems, IoT systems have many devices that can be scattered across various locations, and devices can be in environments that makes them vulnerable, either physically and/or in terms of their network connections. In addition, IoT systems need to be easy to re-configure because of changing technology and applications. For these reasons, it is good practice to always know the current state of each IoT device and the software it contains, as well as to have secure mechanisms for giving remote instructions, including changed parameters, to the devices and for updating their software.

4.1 Device operations and updating

In order to ensure easy updating and re-configuration of IoT systems, a secure mechanism for updating the software in IoT devices is essential. To reduce the costs of updates, IoT software should be written in modules and with parameters and settings that can be remotely updated. The ability to change only parameters or only individual modules minimizes updates and allows those updates that are required to be implemented in a more granular manner, thus reducing telecommunications and other costs.

Two important technological solutions to device management and updating include:

i. A message broker (there is one in the MQTT protocol described in chapter 3.1.2) which acts somewhat like a trusted third party. A message broker enhances security because the broker only receives messages from authorized “publishers”. Then, IoT devices “subscribe” to the broker and periodically request from the broker information that they have “subscribed” to receive (i.e. distribution works on a pull and not a push basis). For software updates, a message broker can send an address for a software update (instead of sending the entire update) which the IoT device then accesses in order to download it.

   Message brokers simplify management, in particular through the use of asynchronous communications, so that if an IoT device is temporarily out of service, or busy, it will still receive the message or update when it comes back on-line or is able to update – and the message broker keeps track of which "subscribers" have received the message and which not. There is also no need to keep a central list of all devices to be updated- they are registered with the message broker as "subscribers" at the time of installation.[17]

ii. The design of IoT software and updates to implement idempotency[18]. This means that when an action is repeated, the result is always the same as when it was implemented the first time. For example, if the same software update or parameter change is accidentally done twice (or even 100 times) on the same IoT device – the result is always the same.

Many elements in IoT architectures rely on open-source software components which means that security vulnerabilities are often fixed quickly. At the same time, in the period between the vulnerability being discovered and the patch being applied, the device is susceptible to the vulnerabilities. This makes particularly important the systems and speed with which IoT devices can be updated.

When designing systems for the management of IOT ecosystems it is also important to keep in mind the need to:

- Design and update, based on experience, **incident management models** for IoT ecosystems. Standards for incidence management for IoT ecosystems do not yet exist – but one can be sure that there will be incidents as real-life operations never run perfectly. In addition, there are no standards for IoT incident management when it is used with for block chain technology, nor guidance on how existing incident management models might be applied to these technologies. There are only generic standards for information sharing such as ISO/IEC 27010, 20614, 20247 and 19592[19]
- Take into account legal considerations when designing the activities of collecting, retaining, analysing, deleting, and sharing data (see chapter on Legal Challenges in Section III).

Device State Monitoring

In addition to a mechanism to update the software in an IoT device, a mechanism is needed to correctly know the state of that IoT device. This means as a minimum, a log showing the current software configuration as well as past software configurations, a software operations log and the communications status of the device.

[17] https://www.ibm.com/cloud/learn/message-brokers# (accessed 12-10-2020)

[18] https://medium.com/@ahmadfarag/idempotency-764f7bb6e4e2 (accessed 12-10-2020)

[19] IS/IEC 27010 - Information Security management for inter-sector and inter-organizational communication

ISO 20614 – Data Exchange protocol for interoperability and preservation, ISO 20247 – International Library Item Identifier, ISO 19592 – Security Techniques – Secret Sharing

4.2 Device Security and Audit

Because IoT data can be used to make decisions (for example, to pay an insurance claim or not) and the data can be used for developing AI inference models or for smart contracts on blockchain networks, there is frequently a need to guarantee that the data is true and is from the real world.

Technical solutions to support this guarantee include:

- **Network Security**
  In communication between a device and a system, or between devices, security measures for network vulnerabilities are generally provided by placing a firewall around the IoT network (i.e. extra security for communications passing the firewall) and encrypting communications.
- **Device Identity**
  The receiver of data from the IoT device must verify that the sender is the correct partner. This is usually done through public-private key cryptography for communicating device identities. To make this even more secure, in the future, the use of blockchain mechanisms for issuing public-key certificates may become common place.
- **Software Audit**
  Although impersonation can be prevented through the use of device identities, it still leaves the possibility of unauthorized data being transferred due to tampering with a device's software. This can be prevented via continuous auditing and recording of the state of the software in the device. For example, periodically hashing[20] the software in the device (software is just a set of numbers, so you can hash it as though it were one very big number) and recording the hash in a blockchain where it cannot be changed. Then, any time there is a change in the hash, it can be compared to the device log to see if the new hash matches the expected result from an update. For additional security, software audits can be run in **Trusted Execution Environments** which use both hardware and software to isolate a software programme from external interference.[21]

[20] For a definition/description of hashes: https://techterms.com/definition/hash (accessed on 12-10-2020)

[21] https://blog.quarkslab.com/introduction-to-trusted-execution-environment-arms-trustzone.html (accessed 12-10-2020)

5 Complementary Technologies

5.1 Artificial Intelligence (AI)

Artificial Intelligence (AI) is becoming an essential part of many IoT systems as data and system owners seek to use and make sense of large volumes of IoT generated data. In addition, AI when combined with IoT data can provide a range of benefits to trade facilitation, particularly in the area of risk analysis. For example, it could allow shippers and insurance companies to determine which shipments are at the greatest risk of having been damaged or tampered with. It could also support comparative analyses of shipping routes and methods that, previously, were not economically feasible.

AI works by using feeding “deep learning” processes with very large volumes of data (big data) which it uses to develop “rules” for evaluating new data. These rules are called an “inference model” and the model can be updated as deep learning processes receive and analyse additional data.

Deep learning is very computationally intensive, requiring significant computing power and resources. Application of the inference model is much less resource intensive.

As result, in more advanced IoT systems that use AI, decentralization of workloads can be seen. In other words, deep learning takes place on the cloud or another centralized platform and then the resulting AI inference models are deployed onto IoT edge-computing devices to “make decisions” (for example to identify defective products). These edge-computing devices and their AI models can also perform a preliminary evaluation of new data before it is sent onwards for use in further “deep learning”, thus reducing the burden on the cloud AI processing side.[22]

If the data collected by IoT is subject to privacy regulations, one way to ensure the respect of privacy rules is to use federated learning in AI which consists of different techniques for maintaining the privacy of data through local processing and/or encryption.[23]

---

[22] https://blogs.gartner.com/paul-debeasi/2019/02/14/training-versus-inference/ (accessed 12-10-2020)

[23] https://towardsdatascience.com/how-federated-learning-is-going-to-revolutionize-ai-6e0ab580420f (accessed on 12-10-2020)

And https://www.steatite-embedded.co.uk/what-is-ai-inference-at-the-edge/ (accessed on 2021-30-01)

And https://simpliv.wordpress.com/2018/08/14/what-is-ai/? (accessed on 2021-30-01)

5.1.1 Some steps in preparing and saving data for use in AI

Most of the data acquired by IoT for monitoring, operations or other purposes can be considered time-series “big data”. Thus, the data has potential for AI and machine learning uses even if that was not the original purpose for which it was collected. As the cost of AI declines, companies will increase their use of AI and this will increase the value of existing, older data sets. As a result, even if a company is not using AI to analyse its IoT data today, it may want to consider storing its IoT data in “AI friendly” formats for possible use in the future.

To do this, two considerations need to be kept in mind.

The first is how to continuous collect data in a state which would allow its processing in the future. Two possible technology solutions for storing large quantities of data for future use are:

- **Data lakes**[24]: data storage that accumulates raw data acquired by IoT
- **Data marts**[25]: data storage that stores data extracted and processed from the data lake for a specific purpose or subject area

The second consideration is preparing AI data for processing. For this, two commonly used technologies are **MapReduce** and **Stream Processing.**

- **MapReduce** is an open source big-data programming model that supports **parallel computing** – i.e. computation on the same “problem” undertaken simultaneously on a cluster of computers to speed up processing and analysis. It is common to utilize MapReduce processing to create structured data needed for AI and save the results to a data mart (see above) for use as AI learning data.[26]
- **Streaming data** are data continuously generated and including a time stamp. The process of generating streaming data is referred to as **stream processing** and it can be done through AI inference (to pick out data of interest), or it can be as simple as showing an alert if a certain value exceeds a threshold.[27]

---

[24] https://www.forbes.com/sites/bernardmarr/2018/08/27/what-is-a-data-lake-a-super-simple-explanation-for-anyone/#7122bc1b76e0 (accessed 11-10-2020)

[25] This reference also contains a nice table comparing a data lake, data mart, data warehouse and relational database https://searchdatamanagement.techtarget.com/definition/data-mart (accessed 11-10-2020)

[26] https://medium.com/edureka/mapreduce-tutorial-3d9535ddbe7c (accessed on 12-10-2020)

[27] https://medium.com/stream-processing/what-is-stream-processing-1eadfca11b97 (accessed on 12-10-2020)

5.2 Blockchain Technology

What is it? Blockchain technology enables separate parties to place a higher degree of trust in a transaction because the entries in an electronic ledger (database) cannot be easily falsified (i.e. once data is written it is extremely difficult to change, keeping in mind that veracity depends on the data being correct from the outset). This 'immutability' is due to a combination of factors as described in the UNECE Whitepaper on Blockchain in Trade Facilitation[28] which provides a detailed overview of the technology.

As a result of these qualities, blockchain systems can be used as an independent umpire in processes that might otherwise expose participants to the risk of one party not living up to its contractual obligations (counterparty risk) and where third-party guarantors are reluctant to intervene and assume part of that risk.

An additional feature of many blockchains that makes IoT/blockchain combinations attractive as a trade facilitation solution is the ability to implement "smart contracts". Smart contracts are programmes that automatically execute once a set of agreed conditions are met, guaranteeing rapid implementation with minimal human interaction (and thus, often, lower costs). For example, an IoT device communicating GPS coordinates to a blockchain may trigger recognition in a smart contract that a shipment has arrived. This, in turn, may trigger an automatic payment. This decision-making automation results in faster execution while reducing human handling, and the potential for error and/or fraud. In addition, the use of blockchain technology has the advantage of providing a transparent and auditable information trail.

To take advantage of the tamper resistant nature of distributed ledgers, it is necessary to make direct entries from the IoT devices that are the source of the data (or their IoT gateways).[29] This is to protect the generated data from being suspected of alteration (by an intermediate system). **
Limitations to the use blockchain are well documented. Those most relevant to the use of IoT with blockchain technology include:

- The need for quality data : 'garbage in, garbage out' – this concern needs to be accounted for in overall system design, although it can be partially alleviated by using blockchain smart contracts to evaluate the quality of data before they are written to a blockchain.

[28] https://www.unece.org/fileadmin/DAM/trade/Publications/ECE-TRADE-457E_WPBlockchainTF.pdf (accessed 3 February 2021)

[29] https://www.ibm.com/blockchain/iot (accessed on 12-10-2020)

- Security: standards are immature for platform configurations that support the shared use of software by multiple users who each have access to only their own data (multi-tenancy). For example a logistics cloud system that uses IoT, among other technologies, to collect data about tens of thousands of containers in their journeys from expeditors to destinations but only allows the owner of a container to access and manipulate data about their container.
- Privacy: this requires examining how to protect the privacy of data generated by IoT devices and written to a blockchain that is shared with multiple stakeholders- this can be done but needs to be incorporated into the original system design
- Inter-ledger interoperability: Where more than one blockchain solution exists (for example, one used by a shipping chain, one used by the bank for trade financing and another one used by customs for AEO status verification) if these blockchain systems cannot 'communicate', then information may still be in silos which require "work arounds" to overcome.

The introduction of IoT has been a boon to trade facilitation because it has generated hitherto untold volumes of granular data on trade – surpassing by far previous manual data collection systems. Nonetheless, gaps in data remain, and where there are gaps, or distortions or inaccuracies, these shortcomings remain an issue in the data registered on a blockchain. In addition, unless a blockchain's governance , or smart contracts, dictate otherwise, blockchains are data takers, recording all the trade data they receive, without any analytical selection process. This could be an issue if all the data coming from an IoT ecosystem were written to blockchain, because the sheer volume of data generated could cause system failures, or cost hikes on networks that charge a small fee each time data is written to a blockchain.

This is why, although IoT devices can be a useful way to capture data; generally, not all IoT data is written to a blockchain. Data from IoT devices is often filtered so that:

- Only data that goes outside of defined ranges is communicated, or
- The data is communicated as a total set of readings at the end of a process, or
- A "hash"[30] of a large volume of data gathered over a precisely defined period is saved on the blockchain while the data itself is saved elsewhere. This last option works because if you want to verify the data, you put it through the hashing mathematical functions and if the result is different than the result saved on the blockchain, then the testing party knows that the underlying data has been changed.

[30] A "hash" is a sort of cryptographic fingerprint that changes if even one character in the "hashed data" changes. So there could be a gigabyte of data and if even one digit, or one space, in that data is changed, then the hash for the entire gigabyte of data will change. The process cannot, however, be used to identify where the change was made.

5.2.1 Advantages of combining IoT and Blockchain for Trade Facilitation

The core of any IoT ecosystem is the orchestration of data flows. In other words, the interactions between data, and its routing, as data comes to and goes from IoT devices including interfaces with edge-computing and gateway devices, the cloud, databases/blockchains and operations and/or analytical software applications (including smart contracts registered on a blockchain).

The technical aspects of this orchestration are considered above. This and the next two chapters looks at factors to consider when evaluating the value addition from deploying blockchain technology in an IoT ecosystem, taking into consideration its strengths and weaknesses and concludes with a few examples of how IoT is already being combined with blockchain to create improved trade facilitation.

As discussed in the introduction, trade facilitation is "the simplification, standardization and harmonization of procedures and associated information flows required to move goods from seller to buyer and to make payment[31]". Trade processes are characterized by a high volume of repetitive activities and transactions, carried out by a large number of stakeholders – textbook conditions for the use of both IoT and blockchain technology with the advantages for trade facilitation that are described below.

Simplification

IoT used in conjunction with Blockchain, and particularly the use of smart contracts, can simplify processes by removing intermediary actors whose primary purpose was to ensure the authenticity of data and/or to request action based on that data. Now the data can come from IoT devices, the "requests" for action can come from an IoT ecosystem and/or a blockchain smart contract and the authenticity can be ensured via registration on a blockchain.

Standardization

Blockchain supports increased confidence in shared (or common) data provided by IoT ecosystems via its ability to:

- Facilitate a common understanding amongst stakeholders; for example, shipping and receiving companies or a trade financing bank and an exporter. For example, stakeholders can access and use the same, verifiable data to describe objects/events related to containers, if the containers have

[31] Trade facilitation implementation guide, available at https://tfig.unece.org/details.html (accessed on 14-08-2021)

installed IoT devices or IoT readable tags/codes such as NFC, RFID or QR codes[32]. These can be read by other IoT devices, and selected information stored on a blockchain for access.

- Reliably identify the time and origin of every entry from an IoT ecosystem in a blockchain. For example, a trade financing bank could identify exactly when goods arrived at the importers warehouse or an insurer could exactly identify when goods were damaged (and who had possession of them at that moment).
- Verify IoT data with high levels of confidence because of its resistance to cyberattacks due to its use of cryptology.

Harmonization

Blockchain technology used with IoT supports harmonization because:

- All stakeholders with “read rights” for blockchain data, view the same IoT data which is available to all at the same time, thus injecting clarity and increasing the potential for collaboration.
- The same IoT information is recorded on all nodes across the blockchain.
- Blockchain strengthens the integrity of data captured from IoT devices through its high level of reliability. A blockchain cannot verify data (although smart contracts can have a role in verification), however, a blockchain eliminates the risks associated with the single point of truth (single source of data) created when IoT data is recorded on one database.

In addition to high levels of reliability, ‘smart contracts’ are a blockchain feature that makes IoT/blockchain combinations attractive as a trade facilitation solution. Smart contracts are programmes that automatically execute once a set of agreed conditions are met, guaranteeing rapid implementation. For example, an IoT device communicating GPS coordinates to a blockchain may trigger recognition in a smart contract that a shipment has arrived. This, in turn, may trigger an automatic payment. This decision-making automation results in faster execution while reducing human handling, and the potential for error and/or fraud. In addition, the use of blockchain technology has the advantage of providing a transparent and auditable information trail.

[32] **Near-Field Communication (NFC)** enables short-range communication between compatible devices. **Radio-frequency identification** (**RFID**) uses electromagnetic fields to automatically identify, and track tags attached to objects. A **Quick Response (QR)** code is a type of matrix barcode that, in this case, links the reader to a specific URL.

To take full advantage of the tamper resistant nature of distributed ledgers, it is necessary to make direct entries from the IoT devices that are the source of the data (or their IoT gateways).[33] This is to protect the generated data from being suspected of alteration (by an intermediate system).

[33] https://www.ibm.com/blockchain/iot (accessed on 12-10-2020)

5.2.2 Blockchain and IoT Disadvantages

The limitations and drawbacks of using blockchain are well documented. Those relevant to the use of blockchain technology with IoT for trade facilitation include:

- The need for quality data because 'garbage in, garbage out' remains true with blockchains – although this can be partially alleviated by using blockchain smart contracts to evaluate the quality of data before they are written to a blockchain.
- Security standards are immature for platform configurations that support the shared use of software by multiple users who each have access to only their own data (multi-tenancy).
- Data privacy regulations may require examining if data generated by IoT devices should be written to a blockchain that is shared with multiple stakeholders.
- Interoperability between blockchains may not be easy to establish. Where more than one blockchain solution exists (for example, one used by a shipping chain and one used by customs) if these two systems cannot 'communicate', then information may still be in silos.

The introduction of IoT has been a boon to trade facilitation because it has generated hitherto untold volumes of granular data on trade – surpassing by far previous manual data collection systems. Nonetheless, gaps in data remain, and where there are gaps, or distortions or inaccuracies, these shortcomings remain an issue in the data registered on a blockchain.

In addition, unless a blockchain's governance, or smart contracts, dictate otherwise, blockchains are data takers, recording all the trade data they receive, without any analytical selection process. This could be an issue if all the data coming from an IoT ecosystem were written to a blockchain, because the sheer volume of data generated could cause system failures and/or cost hikes on networks that charge a small fee each time data is written to a blockchain.

This is why, although IoT devices can be a useful way to capture data; generally, not all IoT data is written to a blockchain. Some methods for maintaining the ability of a blockchain to make data trustworthy while not writing all data to the blockchain are described in Section I. One example is filtering data so that only data outside of a defined range is communicated. Examples of when selective transmission of IoT data is commonly used include vibration sensing in shipments of sensitive electrical goods, as well as temperature and humidity sensing in shipments of perishable goods or pharmaceuticals.

5.2.3 Two Examples of Using IoT with Blockchain to Facilitate Trade

Temperature Sensing for Insurance Purposes

Fruit is temperature sensitive and is best kept between 4 and 15 degrees Celsius during shipment. If, for example, during transportation an IoT device in a cargo container records that fruit was kept at 0 degrees Celsius for 2 entire days, this can trigger insurance-related actions. In other words, the IoT device transmits temperatures falling outside the range, this information on the blockchain activates a smart contract, which notifies the insurance company that a payment should be made to the exporter to compensate for the goods destroyed by the excessively low temperature. That payment is automatically made by the smart contract without any further intervention by either the importer, the exporter or the transport company. This significantly decreases the cost for insurance companies of processing claims because they do not have to reconcile information submitted by the shipper/exporter with the insurance policy, evaluate the truth of the insurance claim (the IoT data registered on a blockchain provides the proof) and then request payment. In addition, it reduces the costs for the shipper/exporter as they do not have to undertake any further documentation of the problem that occurred, and they receive their insurance payment more quickly.[34]

Trade Finance

The traditional system of trade finance involves the transfer of a Bill of Lading (BoL) to the cargo owner either physically or through email; and matching the BoL data with warehouse receipts of cargo, both of which can be forged, to raise finance. A common form of fraud is issuing multiple warehouse receipts for the same goods and then using these fraudulent receipts to raise financing. IoT can combat fraud by monitoring, in real time, cargo in transit and at the warehouse. Data collected by the IoT devices, written to a blockchain (to prove authenticity), can then be traced by stakeholders with 'read only' access. In addition, as in the previous example, when conditions are met (cargo arrived on time, for example) smart contracts can be triggered to execute trade finance contracts. By providing stakeholders with a secure and immutable source of data, the combination of IoT and blockchain technologies doesn't eliminate fraud, but it does make it harder to commit.

Conclusion: Economic transactions involving cross-border trade depend on access to timely, trustworthy data. IoT devices writing to a blockchain can provide a solution, enabling real-time access to information for users ranging from sellers to buyers and intermediaries such as third-party logistics providers and customs officials. Smart contracts – a feature of blockchain – can act as an automatic reconciliation mechanism,

[34] This example and a more comprehensive analysis can be found in the UNCEFACT White Paper on Blockchain in Trade Facilitation https://www.unece.org/fileadmin/DAM/trade/Publications/ECE-TRADE-457E_WPBlockchainTF.pdf

facilitating the rapid execution of payments against a given set of conditions. In addition, blockchains are relatively resilient to cyber-attacks due to their use of cryptography. While issues of data quality and interoperability are common to both IoT and blockchain, the use of IoT with blockchains can be a highly effective instrument for trade facilitation.

Section II IoT in Trade: Supply Chains and Government Infrastructure Management

6. IoT and Supply Chains

Today, supply chains play a vital role in sustainable economic growth in every industry and region. At the same time, rapid globalisation and the expanding geographic reach of supply chains has resulted in ever-increasing complexity and modern supply chains face numerous challenges such as:

- Coordinating across various geographically disbursed, and often disconnected supply chain actors (producers, brokers, transporters, processors, retailers, wholesalers and, of course, consumers).
- Reacting to unexpected changes in demand and supply-chain configurations such as those created by the COVID-19 pandemic of 2020
- Demands for fast last-mile delivery, accurate delivery times and direct-to-consumer fulfilment (with its direct impact on customer relationships)
- Manual and difficult data reconciliation procedures
- A lack of end-to-end supply-chain transparency, product traceability, and record maintenance coupled with a need for in-depth, end-to-end supply-chain inventory visibility (with instant data access and data security)
- Stock-management issues (back orders, recording stolen, damaged or lost stock, maintaining minimum stock levels, etc).
- Rising costs due to unplanned logistic movements and the unpredictability of freight transportation.

IoT, when combined with other technologies, offers an opportunity to address many of these challenges. Undoubtedly one reason that the vast majority of IoT expenditure is undertaken by businesses looking to improve operational efficiency and find new revenue opportunities.

In a previous Whitepaper on Smart Containers[35], UN/CEFACT has described in great detail the use cases for IoT for in multi-modal transport, so that information, while important for supply-chains is not repeated here.

6.1 How could supply chains benefit from adopting IoT?

The Internet of Things (IoT) is changing the way we look at tracking products and the monitoring of the environments in which they are produced along the supply chain. Some of these new approaches and how they could help address the above challenges are described below.

- **Location management systems**

  In the logistics sector, IoT can be integrated into smart location management systems. These systems call for the incorporation of IoT devices into vehicles and, when appropriate, logistics packages and containers, in order to support systems that track driver activities, vehicle location, and delivery status. Once goods are delivered or arrive at a specified location, a manager can be automatically notified. The resulting real-time data is an invaluable asset in delivery planning and the compilation and viewing of schedules in order to improve location management and streamline business processes. This type of application will become significantly more useful with the widespread adoption of the electronic version of consignment notes which are at the heart of all transport contracts.

- **Improved Inventory Management**

  Inventory management and warehousing are among the most important parts of supply-chain ecosystems. Inventory systems are designed to help supervisors and business owners keep track of the products they have on hand, but there's only so much these systems can do when they rely on manual input and manual hand counts to update inventory numbers.

[35] http://www.unece.org/fileadmin/DAM/trade/Publications/ECE_TRADE_446E_SmartContainers.pdf (accessed 09-10-2020)

The use of small inexpensive sensors can allow companies to easily track inventory items, monitor their status and position and create smart warehouse systems. Such systems can prevent losses and ensure the safe storage of goods, as well as efficiently locate needed items.

- **Improved Supply Chain Transparency and Management**

Consumers are making more environmentally friendly choices and want to know where their products are coming from. One study of 30,000 consumers found that 66% of shoppers were willing to pay more for a product if the company was committed to environmental change and maintained a transparent supply chain[36].

In addition, supply chain transparency has more benefits than "just" attracting eco-conscious customers, it can also help prevent disastrous supply-chain disruptions by highlighting small problems before they become big. Therefore, both companies and their customers want the ability to trace a product's lifecycle – from the origin of the goods all the way to their delivery into the customer's hands.

Transparency requires extensive data collection which can be supported through the use of IoT ecosystems. **Blockchain and IoT technologies when used together** can help fulfil the need for supply-chain traceability, transparency and data security. The placement of radio-frequency identification tags and IoT readers (of RF and other tags) and IoT sensors can allow the monitoring of things such as product temperature and humidity, vehicle location and stages in the transportation process. Using a blockchain-based system, every product can be given a digital ID and information collected about that ID by IoT devices can be securely recorded. The result is information which is secure and available for access by authorized users, using blockchain technology, all along the product lifecycle journey.

- **Real-Time Tracking of Transport Conditions (i.e. Cold-Chain Transport)**

Cold chain transport is an integral part of the supply chain for foods, beverages, pharmaceuticals and chemicals. Globally, between 14 and 30 percent of perishable cargo is destroyed during transit and storage, mainly as a result of unregulated temperatures and poor storage conditions[37]. With extremely sensitive products, like some pharmaceuticals, a temperature variation of fewer than 2 degrees could ruin an entire shipment. The use of IoT can help, by constantly monitoring real-time temperatures during transport and storage, sending alerts if there is any unacceptable variation in a shipment's environment including the interior temperature of trucks or warehouses. Depending upon the product, IoT sensors can

---

[36] https://www.inc.com/melanie-curtin/73-percent-of-millennials-are-willing-to-spend-more-money-on-this-1-type-of-product.html (accessed on 08-10-2020)

[37] https://www.supplychainbrain.com/blogs/1-think-tank/post/29983-how-iot-improves-supply-chain-management also, for food loss due to poor temperature management and storage see the following two studies https://royalsocietypublishing.org/doi/10.1098/rsta.2013.0302 and https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6723314/ and for loss in pharma value chains see https://www.sensire.com/blog/pharmaceuticals-cold-chain (all accessed on 08-10-2020)

also be used to measure other potentially damaging environmental factors such as physical shocks, humidity, air pressure, etc.

- **Advanced and predictive analytics**

The unprecedented volume of data that IoT systems can generate provides companies with the opportunity to gain insights into operations using advanced analytics. The real-time performance monitoring allowed by IoT, creates opportunities for predictive analytics. Predictive analytics is helping companies and corporations create more effective operational strategies and improve decision-making, risk management and much more. One important example of advanced analytics is **predictive maintenance**.

Most warehouses and supply chains have established maintenance schedules, taking equipment offline on a strict schedule to inspect and repair it, in order to minimize damage and downtime from unexpected equipment failures. However, a study by the ARC Advisory Group found that only 18% of equipment failures were due to age. The rest happened randomly, so supply chain owners need new strategies to reduce this remaining, 82% of equipment failures[38].

IoT, combined with predictive analytics, can address this issue. It does so by monitoring the health of each piece of equipment, feeding that data back into management software, and then alerting supervisors and maintenance teams when something needs to be taken offline and repaired - thus preventing costly schedule disruptions and downtime as well as equipment failures.

- **Better contract enforcement and new opportunities for service-level contract clauses**

By allowing constant monitoring, IoT can support contract enforcement and the inclusion of more service-level clauses in contracts. This will allow shippers to better control the implementation of requirements for product storage and establish clear procedures in case of a breach, for example in the form of immediate penalties and/or inspection requirements when storage/transport conditions exceed tolerances.

This additional layer of transparency brings greater value, ensuring that claims are based on data rather than speculation, more clearly identifying responsibilities and allowing shippers to provide more reliable, and thus valuable, product warranties to end customers. In addition, the collection of this data supports

[38] https://www.arcweb.com/blog/proactive-asset-management-iiot-analytics (accessed 09-10-2020)

a wider benefit in the form of a better understanding, and management, of vendor and service provider performance.

- **Fleet Management**

When a business manages a fleet of vehicles — from trucks and vans for deliveries to forklifts and cranes within a warehouse — IoT can help improve the quality of fleet management. As discussed above under advanced and predictive analytics, IoT sensors can reduce costs and improve efficiency by supporting preventative vehicle maintenance. In addition, IoT sensors can support safe and efficient vehicle use by tracking vehicle fuel efficiency and even driver behaviour.

- **Smoother Last-Mile Deliveries**

eCommerce has driven an exponential increase in last-mile deliveries which are among the most challenging because they are time-consuming and costly. IoT can be part of the solution to this problem. GPS together with IoT (for package and vehicle tracking) and real-time traffic analytics (which often uses traffic data collected by IoT devices) can create optimized routes to reduce fuel waste and time spent stuck in traffic. The same asset-tracking technology used in warehouses can also improve consumer package tracking. E-commerce is here to stay, which means last-mile deliveries, and the use of IoT supported delivery logistics will also continue to grow.

- **IoT and Financial services**

Digital insurance services based on IoT technology can support supply-chain activities. By collecting and sharing data through IoT devices, underwriters could achieve better insights into customer behaviours, thus allowing them to better evaluate risk on a real-time basis. For example, and as described earlier, IoT devices can be used to monitor the environment in which goods are transported and stored to ensure the maintenance of their quality.

In addition, data from IoT devices when combined with advanced analysis programmes, including AI and machine learning, can provide « forecasts » of possible losses that may occur during transport, if extraordinary events take place.

- **IoT and Financial operations in supply chains**

Based upon the above-mentioned advantages, improvements and innovations in supply chain processes, this table shows the main supply-chain actors and functions linked to finance, with a description, for each one, of how IoT might be used to support financial functions .

<table>
<tr>
<td>Sellers (receivables, treasury)
- For each production phase: data collection

- Communication of delivery completion status or its updating (e.g. acceptance/ rejection/ other)</td>
<td rowspan="2">Carrier(s)
- At each stage of transport process, updating of the status of the delivery lot (and, if applicable, execution of blockchain smart contracts)

- Communication of delivery completion status (e.g. acceptance/ rejection/ other) including, if applicable, execution of a blockchain smart contract</td>
<td>Buyers' delivery point and supply monitoring
Communication of any IoT monitoring during transport (for temperature, humidity, etc.) that impacts quality of the goods

Activation of lot reception and storage processes at delivery point</td>
</tr>
<tr>
<td>Sellers' dispatching point and supply monitoring
- Order reception and/or dispatching with identification of the delivery lot, recording of data, and updating on a blockchain (if applicable)</td>
<td>Buyers' (payables, treasury)
- Communication of quantity of goods and delivery completion status (e.g. acceptance/ rejection/ other) including, if applicable execution of a blockchain smart contract

- Communication of any IoT monitoring during transport (for temperature, humidity, etc.) that impacts quality of the goods</td>
</tr>
</table>

The above uses of IoT technology, when coupled with blockchain and other technologies, could help fulfil the following financial business requirements:

- Ensure that the quality of goods and the logistics services are aligned with contractual agreements,

- Reduce errors and times in information exchange, ensuring data security, operation tracking, and proper information access for each player
- Ensure the legal validity and feasibility of activities in all phases, also in case of disputes and/or cross-border / jurisdiction environments
- Fully integrate financial players and services in order to create a full end-to-end trade finance process

The final impact of these applications is emerging as better performance in financial activities and related operations, with increased efficiency in treasury and working capital management.

6.2 The Future of IoT in Supply Chains

The use of IoT in supply chains is growing exponentially. The Internet of Things with its sophisticated sensors and communication capabilities makes the invisible visible, transforming supply chains so as to be more efficient and increasingly transparent. When combined with other technologies, IoT can integrate pallets, parts, products, packages, equipment (etc) into one ecosystem where they are continuously monitored, automatically tracked and controlled across networks. The real-time data IoT makes available is paving the way for smarter and more efficient supply chains.

This will lead us toward a future supply chain based on a “don’t touch” philosophy. This means designing all aspects of a supply chain with the intent of reducing, if not eliminating entirely, the manual handling and touching of materials, goods, paper, and data. In the next decade, IoT will become an invaluable tool to keep products moving, regardless of the industry. As we have seen, optimizing asset utilization to drive greater operational efficiency is at the heart of IoT's value proposition in the supply chain. Supply chains and logistics aren't the only industries that could benefit from adopting IoT technology, but this is one industry where it might not be optional for much longer.

7. IoT and Government Services

There are many opportunities for Internet of Things (IoT) use in government, particularly at the municipal level, but also at regional and national levels. IoT applications can help governments provide better and new services to their citizens, in large part by making smarter use of their infrastructure and improving asset management.

For governments, the use of standards in IoT solutions is important to reduce costs and increase efficiency. Research has shown that, just at the city level, municipal governments and their technology partners could squander up to 341 billion USD by 2025 if they do not use standards in their implementations[39]. The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) can contribute to a solid standards “foundation” through the internationally agreed data definitions in its Core Components Library (CCL)[40].

IoT applications have the potential to benefit both governments and the people they serve. The data collected and processed by IoT systems can provide insights which support solutions for improving public sector services and reducing public risks through enriched planning, better facilities management, and enhanced security.

IoT when combined with technologies such as blockchain can provide additional support in addressing the challenges faced by governments as they provide public services. For example, sensors embedded in infrastructure such as buses, trains, and bridges could automatically register the need for maintenance and repair work on a blockchain. Once the data is recorded, it could automatically trigger a request for repair work through smart contracts. Once a problem is recorded through IoT sensors, those same devices can also identify whether the issue has been fixed or not. Such IoT based applications can reduce costs, improve services, and provide greater public safety.

Recent research predicts that the global market for IoT in smart cities will grow at a Compound Annual Growth Rate (CAGR) of 18.1% from $113.1 billion in 2020 to $260 million by 2025[41]. This market growth is mainly driven by government smart-city initiatives and Public-Private Partnership (PPP) models for providing government services.

IoT devices can be used to monitor traffic lights, sound levels, air quality, and water security as well as parking spaces and when public garbage bins are full. A wide range of additional applications also exist, including the tracking of assets, infrastructure management, support to the fight against crime, and the management of emergencies. For example, data from IoT devices, can be used to direct traffic lights so that they stay green on roads when the conditions make this beneficial for the traffic and fuel economy. Or, as already mentioned IoT devices can be used to monitor the physical status of critical infrastructure such as bridges, roads and

[39] “Inquiry into the Australian Government's role in the development of cities”, IoT Alliance Australia, 2017

[40] Core Components, UN/CEFACT, UNECE, 2017, https://unece.org/fileadmin/DAM/cefact/GuidanceMaterials/ExecutiveGuides/CCL-CCTS-ExecGuide_Eng.pdf

[41] **“IoT in Smart Cities Market by Solution”, MarketsandMarkets, 2020,** https://www.marketsandmarkets.com/Market-Reports/iot-smart-cities-market-215714954.html

buildings in order to notify managers when repair work is needed.

By deploying IoT systems, governments can provide better, more timely services through better situational awareness, quicker response times and operational efficiencies. The costs of IoT systems have also reduced over time, providing more opportunities for governments to install IoT supported systems for the better management of government services.

Remote monitoring (in particular, of traffic and parking), network management, real-time location systems, data management, security, and reporting, and analytics are a few of the areas driving demand for IoT supported systems by government[42].

Some of the areas in which IoT supported systems can improve government services are:

7.1 Energy

Governments have a responsibility to efficiently manage their own use of energy, in some countries, they are also responsible for fulfilling the energy needs of their citizens. The environmental impact of inefficient energy utilisation also makes it important for governments to promote and support smart and clean energy solutions as well as energy conservation.

Smart grids are an emerging IoT based solution to this need. They can allocate energy through demand matching and keeping track of energy pricing without any human intervention. By deploying IoT sensors and blockchain technology, these transactions can be tracked at a granular level and charged to customers accordingly[43]. For example, using IoT devices and blockchain technology, a micro-grid with 15-20 houses with installed solar panels can allocate electricity across households and order more energy from the main grid when needed, while also tracking the money each household owes, based on their usage. In the future such systems could also support the establishment of carbon credits for each household, calculate related taxes and provide data to support government energy policy.

IoT devices can also provide an important support to governments efforts to more energy efficient themselves as described in section 7.3.

---

[42] "IoT in Smart Cities Market by Solution", MarketsandMarkets, 2020, https://www.marketsandmarkets.com/Market-Reports/iot-smart-cities-market-215714954.html

[43] "30+ IoT Applications/Use Cases of 2021: In-Depth Guide", AI Multiple, 2021, https://research.aimultiple.com/iot-applications/

7.2 Public Safety and Crises Management

Information gaps and asymmetries in times of emergency often lead to an inefficient response by public authorities. There are often delays between the start of an emergency, the time when affected citizens are able to alert the authorities and the moment when authorities have enough information to respond appropriately. This can create a difficult situation where authorities are forced to choose between waiting for adequate information about an event and risking the welfare of involved citizens; or committing resources which may not correspond to the situation, with a risk of endangering underinformed responders – or which may be unnecessary.

In defined contexts, and particularly when risks are known in advance, IoT applications have the capability to quickly collect and analyse data about an event and determine and quickly identify and communicate the optimal action(s) to those involved in crisis management.

IoT devices can report on early indicators of emergency events and the situation on the ground as they happen by measuring environmental indicators such as smoke in forest areas, rising water levels, the strength of winds and structural stress in structures such as dams or bridges (which may be caused by age or extreme temperatures as well as high water).

Environmental sensors can also identify early indications of “man-made” emergency events such as traffic jams caused by accidents. An interesting example of this is devices that can detect the sound of a gunshot, providing its location, within 10 feet of the incident. By automatically sensing the sound, the system alerts the police, speeding up their reaction, and also makes them less dependent on witnesses to report a crime. Apart from detecting gunshots, several other data points can be collected from other sensors, such as cameras. and databases to identify any patterns in crime at a particular location. For example, once the police started deploying one such solution in Camden, New Jersy in the United States, it was found that 38% of gunshots in a particular location were not even reported.IoT-connected devices can also support better performance by the authorities responsible for tackling an incident. For example, wearables connected to an IoT ecosystem could provide information about firefighters, first responders and police officers from sensors that monitor their immediate environment and an their heart rate, voice volume, and stress levels. Then, based on that information and when appropriate, the system could alert the person in question and/or other respondents for support. In addition, such data could be used for training and handling future situations in order to support better responses.

Some smart cities are embedding smart infrastructure in sidewalks, for example, Bluetooth and Wi-Fi-enabled paving material could send emergency messages or crime alerts to mobile phones within a certain distance. These systems could further be integrated with other connected devices such as cameras or even social media to allow responders to ascertain a better picture of the scene before they arrive.

7.3 City Planning and Government Infrastructure Monitoring

IoT can be used by governments for city planning, and infrastructure design, and control. IoT devices can collect real-time data on factors such as transportation and traffic conditions, water delivery, food delivery, and land use. To analyse complex environments, IoT based systems take this real-time data from IoT devices and combine it with other information, such as data from land registries and available social services, in order to support intelligent decision-making and produce more accurate records.

IoT based systems can provide dynamic road and highway management by providing smart, real-time data on road status, lane closures, travel times, and toll rates.

IoT data can also support smart energy solutions based on the monitoring of power usage by governments. For example, the electricity and heating used by buildings is responsible for about 28% of all greenhouse gas emissions (another 11% that assigned to "buildings" comes from construction)[44]. It is estimated that, "a smart building with integrated systems can realize 30–50% savings in existing buildings that are otherwise inefficient." [45] Thus, government implementation of smart buildings, using IoT devices in existing government facilities, can reduce costs, energy wastage and consumption; lower energy-related emissions, and result in enhanced government sustainability and energy efficiency.

---

[44] International Energy Agency's 2019 Global Status Report for Buildings and Construction, available at: https://iea.blob.core.windows.net/assets/3da9daf9-ef75-4a37-b3da-a09224e299dc/2019_Global_Status_Report_for_Buildings_and_Construction.pdf (Accessed on 14-08-2021)

[45] Jennifer King and Christopher Perry, "Smart Buildings: Using Smart Technology to Save Energy in Existing Buildings", published by the American Council for an Energy-Efficient Economy, available at https://www.aceee.org/sites/default/files/publications/researchreports/a1701.pdf (accessed on 13-8-2021)

7.4 Water Safety

IoT devices can be usefully deployed to support water security and address the challenges surrounding water supply, governance, and consumer needs. As per observations by the United Nations' 2030 Water Resources Group[46], if current water trends continue, demand could outweigh the water supply by 40% in 2030.

IoT systems can help governments to better understand the challenges surrounding water security, equipping them with data to support the setting of priorities, the channeling of resources, and other governance decisions. Water management can be improved by highlighting the contributions from all parties in the ecosystem, some of whom may be directly responsible for water management without being aware of their roles in water conservation. By deploying IoT systems, agencies can better coordinate responses and better analyse the impact of each policy decision through real-time measurements that allow "lean start-up" style testing as well as predictive modelling.

In the past, the focus in better water management has been on increasing water supply when inventories drop. However, as new sources of water dry up, the focus is now on improving the yield from existing sources. One way IoT can improve the yield from these sources is to precisely determine the point when repair is needed to improve yield and to provide a cost-benefit analysis looking at the cost of the repair vs the volume of water saved. Through sensors, water managers can obtain a better sense of water flows, prioritizing improvements even when the improvement needs to take place within individual households that are not directly involved in water infrastructure. In-home leaks result in a tremendous loss of potable water globally. Just in the United State over 1 trillion gallons (3.79 trillion litres) of water are estimated to be wasted every year (an average of 10,000 gallons (37,850 litres) per household)[47]. Stopping or slowing these leaks can support significantly increase yields of potable water.

Over 70% of freshwater is used for agriculture[48], around 20% for industry and the remaining 10% for domestic use[49]. The greatest water conservation can be achieved through monitoring and automating water use. Water conservation can be made easier if IoT applications are used to collect and distribute monitoring

[46] United Nations 2030 Water Resources Group 2020 Report, page 2, available at https://www.2030wrg.org/wp-content/uploads/2020/12/WRG-Annual-Report_2020_Web.pdf (accessed 14-08-2021)

[47] United States Environmental Protection Agency web site: https://www.epa.gov/watersense/fix-leak-week (accessed on 13-08-2021)

[48] World Bank, "Water in Agriculture" available at https://www.worldbank.org/en/topic/water-in-agriculture

[49] https://www.raconteur.net/worldwide-water-crisis-is-looming/ accessed 14-08-2021

information that supports conservation processes. By providing information such as when and where consumers use water and how much in comparison to others, IoT based systems can provide insights, send reminders, or apply rules on the use of showers, pools, or appliances – thus helping to reduce the domestic use of water.

Agribusinesses often irrigate without considering the risk of potential overwatering. These problems can be eradicated through IoT sensors that provide measurements for use in calculating the water needs of plants such as heat, soil moisture, humidity, and land slope.

Thus, governments can improve water management by using IoT data to create better insights into both demand and supply. But information alone is all that is needed because an infrastructure needs to be in place that allows action(s) to be taken based on that information. Some of this infrastructure consists of software, automated machinery and human intervention. Some consists of automated Internet of Things control devices (i.e. devices which receive instructions via the Internet). For example, servo valves can be programmed to automatically shut off pipes on receiving information that indicates a leakage or rupture.

Through improved operations and better insights, government officials can better utilise existing resources and improve operations which could lead to cost-savings and lower environmental impacts as well as, possibly, freeing up capital for other government services.

7.5 Smart Parking

One frequent IoT use case in government services is Smart Parking. In China, smart parking enabled by IoT technologies allows drivers to easily locate free parking spots[50]. Pollution and congestion are created when drivers circle looking for parking spaces. To help address this challenge, China Mobile created Smart Parking pilots using IoT technology in Southeast Guizhou and Yunnan. The solution consists of sensors that detect several smart parking data parameters such as license plates, and parking bay places and combines these with parking guidance, intelligence parking management, and mobile payments for the city. The benefits from use of IoT include a maximum coverage of parking spaces, low power consumption as the IoT systems are designed for a battery life of many years and low costs due to reduced management and maintenance costs.

7.6 Government IoT deployment

One of the major challenges for governments in deploying IoT initiatives is that officials need to create a balance between handling urgent crises and making strategic improvements. Often a lack of support, budget limitations and poor infrastructure are a hindrance to deploying IoT solutions at a wider scale.

The key to resolving these issues is creating a collaborative environment which keeps all stakeholders accountable for information sharing. Blockchain when combined with IoT systems can help address these challenges and also provide security to protect large amounts of data collected through IoT devices through cryptography. The budgeting issues and infrastructure provision can be handled by through the savings created and/or the use of Public Private Partnerships (PPPs).

[50] https://www.iotone.com/case-study/china-mobile-smart-parking/c1006 (accessed on 19-08-2021)

Section III Legal Challenges for IoT in Trade

While IoT makes possible many novel applications with huge potential, the implementation of IoT can also pose legal challenges. This chapter looks at the legal and data privacy concerns which are raised by the ability of IoT ecosystems to continuously collect, process and store data.

IoT ecosystems are a rapidly developing form of infrastructure that generates large amounts of data. Collecting this data and turning it into knowledge is a key feature of IoT ecosystems. In the context of international trade, this can require the ability to collect data in one country, aggregate it with data from other countries, and analyse it in a third country - all of which entails the ability to move data across borders. The exceptionally large amounts of data so collected can result in “big data” which lends itself to various types of analysis.[51] One example of such an application is the use of IoT for the tracking and tracing of shipping containers.

Considering the impact of IoT, it is important to understand the legal aspects that affect this infrastructure and the movement of data via various connected devices and objects in an ecosystem.

8. Data Privacy and Protection

The ever-expanding and ubiquitous character of the IoT raises specific concerns about data privacy and data protection. The IoT has a unique capacity for increasing the volume and variety of information collected about individuals and entities, as well as the speed of its collection.

The increasing digitization, often based on the use of IoT, of industrial sectors such as transportation, manufacturing, agricultural and utilities also means an exponential growth in data collection and processing. The often highly confidential information in data flows generated from the use of IoT in consumer and industrial settings may reveal critical business and personal information over time such as habits, preferences, locations, affiliations, payment patterns, and other information. IoT connected devices are often, by design, discreet and most often lack traditional screen interfaces, which can pose a challenge when obtaining

[51] Meltzer, Joshua P. 2016. Maximizing the Opportunities of the Internet for International Trade. E15 Expert Group on the Digital Economy – Policy Options Paper. E15Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum <http://www3.weforum.org/docs/E15/WEF_Digital_Trade_report_2015_1401.pdf>

informed consent from the "provider" of data is required. The integration of IoT with other emerging technologies such as artificial intelligence, augmented intelligence, mobile computing and, eventually, applications using quantum computation is leading to new applications for data, a redefinition of what is considered personal information and a re-examination of how to address privacy concerns.

Data privacy and protection laws in the IoT context are increasingly being developed and, particularly, in the European Union (EU) jurisdiction. The European Commission (EC), which is the executive branch of the EU that proposes new legislation and monitors its implementation, has been working since 2009 to develop a clear IoT regulatory framework which facilitates the use of the technology while keeping in mind the key issues affecting public trust in IoT, which are privacy, data protection, consumer protection, safety, security and liability.[52]

The General Data Protection Regulation (GDPR)[53] is considered to be the first pillar of privacy reform in the EU as it strengthens privacy rights and harmonises data privacy laws across the region and beyond. Some of the more significant provisions in the GDPR that affect IoT are:

- *Territorial scope* (Article 3)
- *Conditions for consent* (Article 7)
- *Right to erasure often referred to as the 'right to be forgotten'* (Article 17), *the right to rectification* (Art. 16) and *the right to restrict processing* (Art. 18)
- *Right to data portability* (Article 20)
- *Data protection by design and by default* (Article 25)
- *Breach notification to national supervisory authority* (Article 33)

From a regional trade facilitation perspective, the GDPR has attempted to balance the relationship between the EU and foreign corporations. Specifically, foreign corporations need to apply the same rules as European corporations if they are offering goods and services or monitoring the behaviour or personal data of individuals in the EU. One way to transfer personal data abroad is on the basis of an EC 'adequacy decision' establishing that a non-EU country provides a level of data protection that is 'essentially equivalent' to that provided for in

52 Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, Internet of Things – An Action Plan for Europe (2009) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF>

53 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

the EU.[54] The effect of such a decision is to enable the free flow of personal data to that third country without the need for the data exporter to provide further safeguards or obtain any authorisation. In the absence of an 'adequacy decision', international transfers can take place on the basis of a number of alternative transfer tools that provide appropriate data protection safeguards. The GDPR formalises and expands the possibilities for using existing instruments, like standard contractual clauses and binding corporate rules, to meet its requirements. For example, Controllers and processors will be able to use, under certain conditions, approved codes of conduct or certification mechanisms (such as privacy seals or marks) to establish 'appropriate safeguards'.

The second pillar of EU Privacy reform is the proposed ePrivacy Regulation.[55] This regulation was proposed by the EC in 2017 and is still under consideration before the EU Council. The ePrivacy Regulation updates the Directive 2002/58/EC (ePrivacy Directive) to provide a high level of privacy protection for users of electronic communication services and a level playing field for all market players across borders.[56] The regulation aims to safeguard the confidentiality of communications of personal information. It is a *lex specialis*[57] of the GDPR for electronic communications, which means that the regulation particularises the GDPR to the case of electronic communications, adding specific provisions to protect electronic communications that include personal data and adapting the privacy regulations for electronic communications to take into account technological change. The ePrivacy Regulation proposal explicitly includes the IoT under its scope.: It considers the machine-to-machine (M2M) communication between IoT devices (i.e. transmissions of signals between machines over a network) to be an electronic communication service which falls within the scope of the ePrivacy Regulation proposal.[58]

In the IoT context, data privacy and protection laws are also emerging in other jurisdictions. In the United Arab

[54] *Ibid.* Article 45 'Transfers on the basis of an adequacy decision'.

[55] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>

[56] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058>

[57] Lex specialis is a Latin phrase meaning specific statutory interpretation of laws.

[58] Aida Joaquin Acosta, 'IoT International Regulatory Challenges' Ch. 7 p. 203 in C. Cwik, C Suarez, L. Thomson (eds) *The Internet of Things: Legal Issues, Policy, and Practical Strategies* (ABA, 2019).

Emirates, the Dubai Government has introduced the Smart Dubai Plan 2021, which includes an IoT strategy, to encourage governmental authorities to transition to an entirely paperless government by 2021. The implementation of this strategy is planned over four phases during three years.[59] The Telecommunications Regulatory Authority, a governmental entity responsible for regulating telecommunications and facilitating smart transformation in the UAE, issued an IoT Regulatory Policy in 2018[60] and an IoT Regulatory Procedure in 2019.[61] The policy borrows some terminology from the GDPR, including the terms Consent, Data Controller, Data Processing, Data Processor, Data Subject and Personal Data, but does not purport to incorporate the EU regulatory framework.[62]

In Brazil, Decree No. 9.854 established a National Plan for the Internet of Things on 25th June 2019 to promote IoT in Brazil.[63] It focuses on smart cities, healthcare, agribusiness and manufacturing. To support these IoT plans, the General Data Protection Law 2018 is planned to come into effect in 2020.[64] It replaces and supplements a sectoral regulatory framework and creates a new transversal and multi-sectoral legal framework for the use of personal data in Brazil in the private and public sectors. Notably, it includes the right to: access, rectify, cancel, exclude and oppose treatment of data; as well as the right to information and explanation about the use of data, and data portability (see Article 18).

In India, a final and comprehensive version of its Draft Policy on the Internet of Things, first published in 2015[65], is expected. Its objectives include creating an IoT industry of USD 15 billion. Notably, the policy covers, *inter alia*, smart cities, smart water, smart environment, smart health, smart waste management, smart agriculture,

---

[59] 'Mohammed bin Rashid launches Digital Wealth Initiative and IoT Strategy' <https://sheikhmohammed.ae/ar-ae/news/details?nid=25235&cid=>

[60] Regulatory Policy (Telecommunications Regulatory Authority, 22 March 2018) available in English at <https://www.tra.gov.ae/en/about-tra/telecommunication-sector/regulations-and-ruling/details.aspx?category=5fe4556c-418b-424e-80f3-794562fc2e4e&subcategory=410535a3-5e8d-4a46-90f8-3b1cd539430d#documents>; available in Arabic at <https://www.tra.gov.ae/ar/about-tra/telecommunication-sector/regulations-and-ruling/details.aspx?category=5fe4556c-418b-424e-80f3-794562fc2e4e&subcategory=410535a3-5e8d-4a46-90f8-3b1cd539430d#documents>

[61] Regulatory Procedure (Telecommunications Regulatory Authority, 6 March 2019) available in English at <https://www.tra.gov.ae/en/about-tra/telecommunication-sector/regulations-and-ruling/details.aspx?category=5fe4556c-418b-424e-80f3-794562fc2e4e&subcategory=410535a3-5e8d-4a46-90f8-3b1cd539430d#documents>; available in Arabic at <https://www.tra.gov.ae/ar/about-tra/telecommunication-sector/regulations-and-ruling/details.aspx?category=5fe4556c-418b-424e-80f3-794562fc2e4e&subcategory=410535a3-5e8d-4a46-90f8-3b1cd539430d#documents>

[62] IoT Newsletter – May 2019 (JARM, June 9 2019) <http://karmadv.com/2019/06/09/iot-newsletter-may-2019/>

[63] Decree No. 9.854 (25 June 2019) <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm>

[64] Law No. 13.709/2018 (14 August 2018) <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>

[65] Draft Policy on the Internet of Things (Ministry of Electronics and Information Technology, 2015) <https://meity.gov.in/writereaddata/files/Revised-Draft-IoT-Policy%20%281%29_0.pdf>

smart safety, smart supply chain and logistics, smart manufacturing/industrial IoT, IoT enterprise incubation and capacity building. To support development of an IoT industry, the Indian Government also introduced a comprehensive new data protection law in the Draft Personal Data Protection Bill of 2018. Its objective is to: protect the control of individuals over their personal data, identify the rights of individuals whose personal data is processed, create a framework for the implementation of organisational and technical measures in processing personal data, and establish norms for the cross-border transfer of personal data.[66] The Draft Bill emulates the EU GDPR in some ways. For example, in Article 24, the right to confirmation and access is similar to the 'subject access' right in the GDPR. It also makes several departures from the EU framework. For instance, unlike the GDPR where the right to data portability can be invoked only for personal data provided by the individual, under the Draft Bill it can also be exercised for personal data that is generated in the course of the provision of services or use of goods by the data fiduciary. In addition, unlike the GDPR, the right to be forgotten is not a right to erasure; it is only a right to restrict or prevent disclosure of personal data in particular circumstances.

9. Liability Issues

In an IoT system, the interaction between devices and data involves numerous users and entities. These depend upon the implementation in question and can include the device manufacturers, IoT service providers, mobile application developers, retailers and consumers/end-users. Typically, for any one application/function there are multiple entry and exit points for data. A single vulnerability within the IoT systems supporting supply chains can compromise the security of the entire network and allow unauthorised access at multiple levels. Therefore, risk can be high and it is critical to ascertain liability for the security of IoT devices and to determine who in the chain of supply is liable to the user. The hyper connectivity of devices leads to hyper complexity in assessing liability allocation.

Liabilities can be of both civil (inclusive of tort as a civil wrong in common law jurisdictions) and of criminal nature and can include strict liability. Strict liability is a liability that can be imposed irrespective of whether the defendant intended to cause harm or acted with reasonable care. It is primarily used in reference to product liability.

In the EU, product liability rules are defined in the Product Liability Directive (PLD)[67]. The PLD has been there for some time, covering all types of products and including emerging digital technology products, i.e. including

[66] The Personal Data Protection Bill (2018) <https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>

[67] Council Directive on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability For Defective Products (1985) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374>

IoT devices. The PLD assigns liability to producers when defective products cause damages to victims or their property. It defines a strict liability regime, where the victim has to prove the damage, the defect of the product, and that the damage was caused by that defect. The EC has evaluated[68] the PLD and has set up an expert group on liability and technologies.[69] It intends to issue a guidance document to provide clearer definitions of product, producer, defect and damage and make it more relevant to IoT devices. For example, the concept of producer in the case of IoT devices could be revisited to account for the possibility that devices are refurbished, or their features changed outside of the producers' control. The scope of damages may be widened to cover privacy and cyber-security damages in addition to physical and material damages.

The 2017 EC Communication on Building a European Data Economy[70] states a commitment, "to assess whether the current EU legal rules for product liability are fit for purpose, when damages occur in the context of the use of IoT and autonomous systems". The European Parliament also published a report, asking for liability rules for autonomous systems that would consider safety aspects.[71] In 2018, the EC published a communication on 'Liability for Emerging Digital Technologies'[72] which accompanied a document on AI for Europe. This provided a list of liability challenges related to emerging technologies, and also considered a liability framework for cyber-security attacks.

Since technology is developing faster than law, it is important for companies and businesses to protect themselves in cross-border trade where there can be an element of legal uncertainly. To mitigate risk, it is essential for companies and businesses to develop clear contractual expectations, warranties, limitations, and indemnities as well as to obtain insurance to cover potential liability. The integration of best practices into

---

[68] Commission Staff Working Document 'Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products' (2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018SC0157>

[69] Liability of Defective Products <https://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en>

[70] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Building A European Data Economy' COM/2017/09 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A9%3AFIN>

[71] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 14-16 <http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html>

[72] Commission Staff Working Document "Liability for emerging digital technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial intelligence for Europe" (2018) SWD/2018/137 final https://ec.europa.eu/knowledge4policy/publication/european-commission-staff-working-document-liability-emerging-digital-technologies_en> Also see *Id.* note 8, at p. 207

products, software, and operational infrastructures should be considered by companies in order to systematically reduce liability and for quality management.

Software developers may have traditionally been able to avoid liability for vulnerabilities in their products, but a confluence of new realities suggests that this protection may not be sustainable.[73] IoT devices are not software, they are devices with software. However, whether it is the owners of the IoT device performing the function that are legally required to comply with rules for the allocation of liability or exemption or whether liability can be imposed on the device manufacturers will be subject to the assertion of claim, the nature of the vulnerability and the extent of injury and real harm.

10. Data Ownership

The method, structure and analysis of the large data sets that form big data raise interesting issues on data ownership when such data sets are moved to, transmitted to, or interact with other large data systems in an industrial IoT environment. Data ownership and data rights are generally associated with Intellectual Property Rights (IPRs) where a flow of customer data is being collected, processed, anonymised and notified to the data controller for purpose of optimisation. The ownership and usage of data is usually managed by data-use agreements (DUAs).

Agreements about data ownership and control affecting consumers may be under some form of government supervision or oversight, therefore certain industries (like the healthcare industry) may need to comply with a range of statutes and agency rules.

It is important to note that the term ‘data’ should be defined as clearly as possible in contractual agreements between parties. A related term is ‘derived data’ which is the new data generated though analysis of the original data. A DUA should specify the ownership of the derived data and expressly allocate the ownership interest between the parties so that the ownership rights are clear and distinctive, irrespective of any background IPRs. The agreement should also have anonymity requirements which obligate the analyst to analyse only anonymised data sets provided by the data subject. A data subject may also set restrictions in the licensing for distribution and re-distribution of raw data sets when negotiating IoT usage agreements.[74]

---

[73] Richard M. Martinez, ‘Liability and Connected Products’ Ch. 14 p. 411 in C. Cwik, C Suarez, L. Thomson (eds) *The Internet of Things: Legal Issues, Policy, and Practical Strategies* (ABA, 2019).

[74] David Tollen, ‘The Big Data Licensing Issue-Spotter’, Tech Contracts Academy (08 December 2015) <https://techcontracts.com/2015/12/08/the-big-data-licensing-issue-spotter/#_ftn4>

11. Admissibility of Electronic Evidence

There are a number of challenges associated with the collection and preservation of IoT data for e-discovery and using the data as evidence. For example, identifying the IoT systems and devices where relevant data is stored can be difficult given that the initial data creation often takes place in multiple stages (especially when edge computing and/or machine learning is used).

Another challenge is the authentication of digital evidence in legal proceedings[75]. The factors that are considered in evaluating the integrity of digital data include who created the evidence, what processes and technology were used, and what was the chain of custody throughout the entire life cycle of the digital evidence.

12. Dispute Settlement

As the IoT continues to expand its reach, so too will its impact and the need for dispute settlement. Some examples of the impact of the IoT on dispute settlement follow.

- First, conflict is often a by-product of innovation, i.e. the IoT can, itself, generate disputes.[76] For instance, faulty IoT devices can trigger disputes based on product liability.
- Second, the IoT can prevent disputes since automation has the potential to reduce or remove human error.[77]
- Third, as a new source of digital evidence, the IoT can serve as a tool to prove a case.[78] For example, IoT devices can provide increased visibility of parcel and cargo journeys, in addition to providing real-time tracking information.[79] This increased availability of information provides a unique opportunity for counsel and prosecution to argue and prove a case. That said, counsel and prosecution must learn

[75] Lucy L Thomson, 'Mobile Devices: New Challenges for Admissibility of Electronic Evidence', ABA The SciTech Lawyer (29 June 2017) <https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2013/winter_spring_2013/mobile_devices_new_challenges_admissibility_electronic_evidence/>

[76] Ethan Katsh and Orna Rabinovich-Einy, 'Digital Justice: Technology and the Internet of Disputes' (OUP 2017)

[77] *Ibid.*

[78] Samantha V. Ettari, 'United States: Handling Internet of Things Data in Litigation' (Kramer Levin, 17 January 2019) <https://www.kramerlevin.com/images/content/4/6/v3/46579/ Handling-Internet-of-Things-Data-in-Litigation.pdf> accessed 7 August 2019

[79] Manish Choudhary, 'How IOT is Transforming the Industry' (Entrepreneur, 17 April 2019) <https://www.entrepreneur.com/article/332392> accessed 7 August 2019.

> how to extract relevant information effectively while being mindful of the operational and privacy challenges inherent to this new source of digital evidence.[80] In addition, there is little guidance available since there are few written decisions addressing the use and handling of IoT data in litigation or arbitration.

In the resolution of disputes arising from the digitisation of things, such as those that may arise in the context of IoT ecosystems, arbitration offers several important advantages. For example, it offers parties the flexibility to select the location of arbitral proceedings, which is of particular benefit in disputes of a transnational nature (for example: disputes involving IoT devices that have travelled through different jurisdictions, like smart freight containers). In addition, the possibility afforded in arbitration of appointing expert arbitrators means that IoT disputes can have access to specialized expert knowledge and judgment not available in a traditional court of law.

13. Legal Challenges - Conclusion

While IoT technology introduces the ability to design many novel applications in support of trade facilitation, it is critical that solutions be designed to mitigate not only ICT and physical risks but also legal risks such as those related to data security, safety and privacy while ensuring performance, usability and scalability. Achieving this trade off may require the redesign of existing tools and methods to cater to the specific challenges created by IoT ecosystems.

[80] Re Apple, Inc. 149 F. Supp. 3d 341, 364 n.26 (EDNY 2016).