virt·eu

Relevant IoT Regulation and Standards

Produced by **Javier Ruiz Diaz**, Open Rights Group

This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement No 732027

CONTENTS

1. Introduction

Technological innovation in the domain of Internet of Things presents unique challenges, going beyond the typical concerns with privacy and data protection, due to direct engagement with hardware and physical environments alongside issues of software and connectivity. Thus IoT developers must take into account a much broader range of standards and regulations.

The VIRT-EU project surveyed the wider regulatory framework around IoT, documenting relevant standards and regulations. This report presents a map for IoT designers and developers to understand compliance issues and/or the various standards and guidance currently available. Please note that this is a relatively fast moving field and new standards are coming online quite frequently. This survey was completed in the fall of 2017. As such, please use this document as a basis for further research into this area.

Currently there is little IoT specific regulation, but development of IoT devices must take into account many existing laws and can be subjected to a bewildering panoply of standards and frameworks. Despite the lack of direct IoT regulation – on both sides of the Atlantic – there are myriad issues and conflicts in the sector that require intervention. While privacy, security, and consumer trust appear to be key concerns, there are many other issues and concerns that fall under established regulatory frameworks for telecommunications or consumer protection. Interoperability and standards proliferation are also high in the agenda. Like any emerging area, it is likely that IoT will go through a convoluted process of standard setting that will eventually lead to broad system interoperability. As physical devices become networked, we see emergence of significant security concerns that make interoperability difficult, but it is likely that these concerns will not prevent the drive for efforts towards unifying standards.

Technical standards are a critical aspect of the modern world but they are also important for developers for practical reasons. In many cases, working with a particular technology will be the single most important decision a developer may make. This will have implications for who can use this technology and which other systems will work with it. In addition, it may have some broader implications, such as whether the system will be using free or licensed radio spectrum, whether the design can be made available fully open source, or whether a single company will control future technical developments. These questions raise significant ethical considerations but are often difficult to disentangle not least because many developers may not even be aware of the variety of regulations they ought to consider at the outset.

This research was completed by the Open Rights Group as part of the VIRT-EU Task 2.4 “Research on policies and institutional contexts for data identification, collection and analysis in Europe”. The report was created as part of Deliverable 6.3 for the VIRT-EU project by Javier Ruiz Diaz, Open Rights Group. (grant agreement No. 732027).

2. Sector-specific policy considerations relevant to IoT development

2.1 European Policy Making

The regulation of IoT in Europe does not currently contemplate any specific regulations, but there is a lot of activity in terms of research, industry support and standardisation. A consultation in 2013 by the European Commission, for example, concluded that there was no need to provide specific legislation at that stage.[1] The Commission could not reach consensus on whether IoT-specific regulation was necessary. Industry respondents argued that state intervention would hamper the young sector while privacy advocacy groups and academics asked for specific regulation.

2.2 Unit e4 of the European Commission

The European Commission's Unit e4[2] is the centre of competence for Internet of Things (IoT), responsible for the policy, research, standardisation, adoption and uptake of IoT and new business models stemming from IoT. The Unit deals with strategic and policy issues and is currently examining liabilities, platforms and standardisation, while also considering the development of a Trusted IoT label or kite mark.

2.3 The Alliance for IoT Innovation

Collaboration of the Commission with industry is centred in a stakeholder platform run by Unit e4 called the Alliance for IoT Innovation (AIOTI)[3]. The alliance has over 170 members covering all aspects of IoT from large industrial conglomerates to software developers, but not internet companies or the main home standards consortia such as Zigbee, Thread or Z-wave. There is very limited civil society presence.

The AIOTI includes some transversal working groups looking at policy or standards and sector specific working groups for smart cities, wearables, farming and energy, among others. Their policy group rejects the need for new specific regulations on IoT both on pro-business light touch principles and in order to protect early innovations from "regulatory error".[4]

Their current policy recommendations focuses on privacy, security, liability and net neutrality. These are quite generic and mainly based on providing information and capacity building across these areas.

Importantly, on liability, compliance and insurance the AIOTI believes that the current legal framework is enough, despite the challenges brought by IoT. These challenges include: the interdependency of technologies and responsibilities not allowing the identification of root causes, the move to services potentially removing "product liability". Liability is discussed in more detail in the sections below.

Other concerns include free movement of IoT data, access to spectrum, interoperability and numbering, and AIOTI plans to make policy recommendations in relation to these topics in the future. However, given that the alliance has been driven top down by the Commission, it remains unclear how much further independent work will be carried out.

2.4 European Standards

The European Commission is centrally involved in the development of certain standards that have become mandatory across the EU. The 2012 Regulation on European Standardisation (Regulation 1025/2012) sets out the procedures in detail.

After consultations with industry and member states, the Commission issued a request or mandate for standardisation on a specific topic to the European Standards Organisations (ESOs). Around 20% of European standards are developed in this way.[5] Unit e4 leads on IoT standards.

For example, under the mandate M/436 European Commission request that the ESOs deliver a coordinated response on the subject of Radio Frequency Identification Devices (RFID), in relation to data protection, information security and privacy.[6]

The three ESOs are the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI).

The ESOs are the regional mirror bodies to their international counterparts, i.e. ISO (the International Organisation for Standardisation), IEC (the International Electrotechnical Commission) and ITU-T (the International Telecommunication Union, telecommunication standardisation sector) respectively.[7]

The ANEC[8] is a consumer body that represents the voice of consumers on these standards organisations through volunteers that participate in various working groups relevant to IT and IoT[9]. Their role is recognised in the Standardisation Regulation.

The development of mandatory European standards specific to IoT is very limited although these bodies do a lot of work in this area, also as part of international bodies. There are, however, many mandatory telecommunication and electrical standards that apply to IoT devices. These organisations and their roles in IoT are discussed in the sections below on regulations.

The European Commission published an architecture for IoT in 2014, but the initiative does not appear to have been developed further.[10]

2.5 US Regulation of IoT

In order to understand the regulatory framework in Europe it is important to look at how IoT policy is developing in the US, which holds a huge influence on technological issues.

The regulation of IoT in the US also takes a light touch approach. The Federal Trade Commission (FTC) considered their regulatory approach in a 2015 report that considered privacy and security in IoT.[11] The report made some soft recommendations around data minimisation, the need to prioritise security of devices, and how to information and give consumers choice in devices without an interface. However, it concluded that it would be premature to legislate specific IoT regulations at such an early stage, asking instead for stronger general privacy laws to be created.

The FTC has concluded that "while the Internet of Things has several unique practical challenges in privacy and data security … the legal framework that surrounds it is for the most part the same as the legal framework that applies to other types technology."[12]

The US Senate has introduced the Developing Innovation and Growing the Internet of Things Act or the DIGIT Act,[13] which would require the US Department of Commerce to convene a working group of federal stakeholders to provide recommendations and a report to Congress regarding the IoT.

The Federal Communications Commission is opening spectrum[14] as part of an Innovation drive that includes promoting IoT, and also includes and new a Citizens Broadband Radio Service (CBRS) that opens up wireless frequencies from 3550MHz to 3700MHz to new users. However, it is unclear which devices will operate in these frequencies.[15]

2.6 China

China is a key player in digital technology and IoT in particular.[16] Chinese companies such as Huawei are part of many IoT consortia and provide infrastructure, while most electronics are manufactured in that country. China has more connected devices than any other country.[17]

The Chinese government has strong industrial strategies – particularly for smart manufacturing in their Internet+ strategy – and has produced various enabling pieces of legislation for internet security.[18] China is strengthening its internal standards compliance and increasingly participates in standardisation bodies.

The Internet Security Law 2017 imposes data localisation, with personal data not being allowed to leave China, and other restrictions on scientific or technological data.[19] This could be an issue for IoT developers wishing to enter Chinese markets.

A more common issue for IoT developers will be managing their relations with Chinese manufacturers. This can be a very problematic area, and specialist IP lawyers tend to single out IoT developers as especially naive in giving their rights away.[20]

China is the main innovation hub for Internet of Things developments, apparently unfazed by privacy and data protection issues, other than localisation. At the regulatory level, however, it does not have the influence of the EU or US

[1] Conclusions of the Internet of Things public consultation. (n.d.). Conclusions of the Internet of Things public consultation. Retrieved November 27, 2017, from https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation

[2] Internet of Things (Unit E.4). (n.d.). Internet of Things (Unit E.4). Retrieved November 27, 2017, from https://ec.europa.eu/digital-single-market/en/content/internet-things-unit-e4

[3] The Alliance for the Internet of Things Innovation. (n.d.). AIOTI – SPACE | The Alliance for the Internet of Things Innovation. Retrieved November 27, 2017, from https://aioti.eu/

[4] Report AIOTI Working Group 4 – Policy. ALLIANCE FOR INTERNET OF THINGS INNOVATION. aioti.eu, 2015. https://aioti.eu/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf

[5] Standardisation requests – mandates – Growth – European Commission. (n.d.) Retrieved November 27, 2017, from https://ec.europa.eu/growth/single-market/european-standards/requests_en

[6] Dessene, G. (n.d.). Mandate M436 – Information and Communication Technologies applied to Radio Frequency Identification (RFI. Retrieved November 27, 2017, from http://www.centrenational-rfid.com/docs/applications-rfid/cnrfid%20gerard%20desenne.pdf

[7] CENELEC – About CENELEC – Who we are – European partners. (n.d.). Retrieved November 27, 2017, from https://www.cenelec.eu/aboutcenelec/whoweare/europeanstandardsorganizations/

[8] Who we are – ANEC: The European consumer voice in standardisation. (n.d.). Retrieved November 27, 2017, from https://www.anec.eu/about-anec/who-we-are

[9] Digital Society – ANEC: The European consumer voice in standardisation. (n.d.). Retrieved November 27, 2017, from https://www.anec.eu/priorities/digital-society

[10] European Commission. (2014, June 2). Putting interoperability into the Internet of Things | Digital Single Market. ec.europa.eu

[11] Internet of Things: Privacy & Security in a Connected World. (2015). Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[12] Who's in Charge of Regulating the Internet of Things? (n.d.). Retrieved November 27, 2017, from http://www.nextgov.com/emerging-tech/2016/09/internet-things-regulating-charge/131208/

[13] DIGIT Act, S.2607, 114th Cong. (2016)

[14] Goovaerts, D. (2017, August 10). FCC Looking Into Use of 900 MHz Band for Broadband, IoT. Retrieved November 27, 2017, from https://www.wirelessweek.com/news/2017/08/fcc-looking-use-900-mhz-band-broadband-iot

[15] Thornycroft, P. (2016, January 28). FCC's 3.5 GHz 'innovation band': What kind of networks can we expect? Retrieved November 27, 2017, from https://www.networkworld.com/article/3027162/mobile-wireless/what-can-we-expect-from-the-new-lightly-licensed-35-ghz-band.html

[16] GSMA. How China is scaling the Internet of Things. (2015, July). Retrieved November 27, 2017, from https://www.gsma.com/newsroom/wp-content/uploads/16531-China-IoT-Report-LR.pdf

[17] Asia Pacific will Dominate the Connected Device Market, Fuelled by Explosive Growth in China, says GSMA – Newsroom. (2011, November 16). Retrieved November 27, 2017, from https://www.gsma.com/newsroom/press-release/asia-pacific-will-dominate-the-connected-device-market-fuelled-by-explosive-growth-in-china-says-gsma/

[18] Dongyang, F. (n.d.). IoT Security Policy and Regulation Initiatives in China. Retrieved November 27, 2017, from https://docbox.etsi.org/workshop/2016/201606_SECURITYWS/S04_POLICYandREGULATORYINITIATIVES/CHINA_HUAWEI_DONGYANG.pdf

[19] Internet Security Law of the People 's Republic of China. (n.d.). Retrieved November 27, 2017, from http://bit.ly/2iV405c

[20] Harris, D. (2016, March 27). China and The Internet of Things and How to Destroy Your Own Company |. Retrieved November 27, 2017, from https://www.chinalawblog.com/2016/03/china-and-the-internet-of-things-and-how-to-destroy-your-own-company.html

3. Global Standards Bodies for IoT

The Internet of Things involves telecommunications and electronics technologies that are generally standardised at the international level by a handful of institutions. As discussed previously, there is proliferation of standards specific to IoT deployments, but underneath these there are also standards for general technologies used by IoT.

This section describes the main global standards bodies involved in regulating the field of electronics, telecommunications, and the internet, and highlights some of their specific programmes and activities around IoT.

These bodies tend to operate at the middle and lower layers of the OSIO model. Developers will rarely make design decisions that directly involve these, as they generally operate a higher level, but the technologies they use will have been developed in these contexts. The one exception is designing systems to use mobile telephony, as this has far-reaching practical implications for the use of personal data. 3GPP and GSMA are responsible for the standards around mobile telephony.

Although developers may not be fully aware of the processes through which the technologies they rely on are formed, these can have important implications. Decisions about encryption for example have moved from the OSI presentation layer discussed above to lower elements of networking, and every protocol or standard will have its own approach to security and the management of data.

All of these bodies have a working group or similar arrangement looking at IoT, but the depth and breadth varies considerably. It seems that all these bodies wish to carve out some space in IoT. In some cases, this has taken the form of hosting existing industry standards, such as with Z-wave and the ITU, while in other cases they contribute to wider IoT efforts such as OneM2M.

These global organisations also take input and have working relationships with their regional or national members. The roles of European Standards Organisations are explored in other sections about specific regulations, but it is worth noting their close relation to ISO, IEC and ITU.

It would be fair to say that those, more traditional and bureaucratic, organisations have moved more slowly in relation to IoT, which is understandable. This has been an issue throughout the development of most modern telecommunications since the 1970s. In contrast, more nimble organisations such as the Institute of Electrical and Electronic Engineers (IEEE) and the Internet Engineering Taskforce (IETF), have developed open standards that are widely used in IoT.

Other standards groups such as the OASIS are certainly less relevant to IoT. Currently, they may carve out a space by collaborating with existing industry groups, but it is unclear what their role would be in the long term.

The World Wide Web Consortium (W3C) is in a very particular position. Modern IoT and home automation technologies are moving in the direction of increased compatibility with established Internet and web standards. This should give the W3C a larger role in IoT.

3.1 ITU

The International Telecommunications Union (ITU) is the United Nations specialised agency for information and communication technologies – ICTs. It allocates global radio spectrum and satellite orbits, and develops various technical standards. The ITU traditionally represents a model of technology governance based on strict government regulation that has been fiercely opposed by many actors in the internet world, who instead support a multi-stakeholder regulatory model. However, the ITU has broad support among developing nations and could be important in spreading future standards. ITU has also produced key recommendations for telecoms technologies such as ADSL.

Until 2015, the ITU-T (its standardisation branch) ran a Global Standards Initiative on the Internet of Things (IoT-GSI) focused on developing "the detailed standards necessary for IoT deployment, taking into account the work done in other standards development organisations (SDOs)." [21]

Since then, work at the ITU has moved to *ITU-T Study Group 20 – Internet of Things, smart cities and communities,*[22] which continues to work on standardisation. Their programme of work covers many areas from transportation to sensors, and their approach focuses on infrastructure and interoperability, mainly from the perspective of city platforms. The group also has an extensive programme of work on the oneM2M standard discussed elsewhere.

The ITU maintain the specification for the standard ITU-T G.9959: *Short range narrow-band digital radio-communication transceivers*[23] – that provides specifications for various layers including the lowest levels, and was originally developed for the Z-Wave technology discussed below.[24]

3.2 ISO/IEC

The International Organisation for Standardisation (ISO) is an independent, non-governmental international organisation with a membership of 162 national standards bodies. Based in Geneva, like the ITU, ISO represents the closed, top down standard model that the internet has shaken to its core in the past decades with its open approach.

ISO has developed various standards related to IoT[25] – mainly around sensor networks – under its technical committee "JTC 1 Information technology" and a draft Reference Architecture[26] for IoT.

ISO works with the International Electrotechnical Commission (IEC) in the development of these standards. Founded in 1906, the IEC (International Electrotechnical Commission) is the world's leading organisation for the preparation and publication of International Standards for all electrical, electronic and related technologies.[27] IEC has various work streams on smart cities, grids and other electrical related issues that address the IoT. For example, the ISO/IEC 18000 series of standards define diverse RFID technologies.[28]

In addition to the ESOs discussed elsewhere, national standards organisations, such as the British Standards Institution (BSI), are members of ISO and can publish their own standards and later on possibly promote these for global adoption. The BSI for example has published *PAS 212, Automatic resource discovery for the Internet of Things – Specification*.[29] The specification has been developed in conjunction with the Hypercat Alliance[30], supported by public funding from Innovate UK and backed by a number of businesses and public sector organisations. The standard is so far British in scope, but the ambitions of the alliance are clearly for it to become a global standard.

3.3 Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE) is an international organisation with over 400,000 members that aims to be "the trusted "voice" for engineering, computing, and technology information around the globe". [31]

The IEEE is the most important body standardising protocols and technologies used today that operate at the lower layers of the OSI model. These include 802.11 (Wi-Fi), 802.15 (Wireless Personal Area Networks, which include Bluetooth), and 802.16 (broadband wireless), 802.3 (Ethernet), and 1901.2 (power line networks).

IEEE also developed and maintains standards that are quite specific to IoT applications. IEEE 802.15.4, the technical standard for low-rate wireless personal area networks (LR-WPANs), is the most important standard for such low range low power networks and forms the basis for many more specific standards, and it is used by the popular Zigbee and Thread protocols for connecting consumer appliances. This protocol also adds encryption and security at the low data link layer, evidencing the concerns about these issues in IoT.

IEEE has also published a draft standard (P2314) on an architectural framework for the IoT, incorporating several hundred IEEE standards applicable to IoT.[32]

The institute has an extensive range of work on IoT from running courses to developing a long list of standards, mainly for telecommunications, from low power range, sensors and city-wide networks. In addition, they have sector specific standard for health and smart grids among others.[33]

3.4 Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is the leading Internet communications standards body. It is a "large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual."[34] The IETF generally publishes a type of document called a Request for Comments (RFC), to stress the dynamic and open nature of its work.

While the IEEE discussed above generally deals with the low-level data link connectivity of a specific network, the IETF works on the internet proper at the medium and upper layers of the OSI model. The IETF maintains the basic Internet Protocol (IP) that runs the internet and its newer version IPv6, which is very important for the future of IoT as the current version is reaching the limit of unique addresses it can provide. IETF has several working groups developing standards related to IoT[35] mainly working on low power and low bandwidth networking

The 6LoWPAN standard (IPv6 over Low-power WPAN) takes IPv6 and compression and optimisation techniques to very small devices with limited capacity radio links. This standard is mainly based on IEEE 802.15.4 wireless standard but can also be used over wifi or even Ethernet, and provides a high level of compatibility with the internet through simple bridging devices.

The Thread home automation protocol discussed below is based on 6LoWPAN. The Zigbee standard group has introduced Zigbee IP as an IPv6 protocol also based on 6LoWPAN.[36]

The IETF also maintains the Constrained Application Protocol[37] (CoAP) specialised protocol for applying modern web technologies (http and RESTful) to small and limited IoT devices, and it is natively compatible with the Internet.[38] This standard operates in the higher OSI layers and it is a direct alternative to the older MQTT, maintained by OASIS and discussed below. More recently the IETF has taken a strong interest in security, with various working groups and projects geared to strengthening encryption in low power devices.

3.5 OASIS

The Organisation for the Advancement of Structured Information Standards (OASIS) is a non-profit consortium that maintains global open standards through industry consensus, including the Open Document Format (ODF) for word processors.

OASIS includes IoT in their areas of work, but in practice this is quite limited. The consortium maintains the MQ Telemetry Transport (MQTT) standard,[39] originally designed by IBM for satellite communications with oil-field equipment.[40] This standard has now been approved by ISO/IEC as well.[41]

This is an important standard for business applications but less relevant for consumers. The newer CoAP standard from IETF provides a similar function.

World Wide Web Consortium

The World Wide Web Consortium (W3C) is responsible for standards at the top layers of the OSI model that form the web. The web has evolved since its inception towards increasing levels of automation and machine to machine communications to form complex web applications and services. The widespread use of Google Docs or similar systems is a visible part of this drive.

The W3C has a Web of Things Working Group – chaired by engineers from industrial groups Panasonic, Intel and Siemens[42] – that has recently published its first drafts. The consortium's stated objective is to reduce fragmentation through royalty-free platform independent standards.[43]

While they are at a very early stage, the W3C could become important. There is a drive toward compatibility with internet and web technologies, such as in the CoAP protocol. Direct interaction of IoT devices with users via web technologies would seem natural, given that this is how most people face technology nowadays. In addition, many newcomers to programming learn mainly web technologies that work at the higher OSI layers and completely abstract interactions with hardware or lower networking protocols.

3.6 GSMA / 3GPP

Modern mobile telephony industry standards are mainly hosted by the 3rd Generation Partnership Project (3GPP)[44]. This is a sector where technology and standards are particularly driven by industry, with mobile telecoms providers enjoying a very strong political position as payers of large sums to governments in spectrum auctions.

The global mobile industry association GSMA works with its members to drive standardisation through 3GPP and also in other bodies. GSMA is a key player in many standard and policy spaces, but it has not published standards itself, focusing instead on guidelines towards practical applications, e.g. Security,[45] or specifications.[46] The association also has important role in the development of the embedded SIM cards that allow quick remote change of providers or roaming.[47] 3GPP also carries out some IoT specific work, such as connected cars in the Cellular Vehicle-to-Everything (Cellular V2X) standard developed with GSMA.

The mobile industry will naturally want to subtly promote IoT networking models that rely on the use of GSM mobile telephony and 5G, where these companies have control of the spectrum as opposed to newer low power long range technologies that can use freely available spectrum.[48] The use of the mobile telephony system by IoT developers – instead of open technologies – will have an important impact on data privacy and the possibilities for government surveillance.

3.7 CEPT/ECC

The European Conference of Postal and Telecommunications Administrations – CEPT – is a cooperative body in Europe of 48 national regulatory administrations. It was established in 1959, originally by the state monopolies in these areas. CEPT's activities include "co-operation on commercial, operational, regulatory, and technical standardisation issues".[49]

The Electronic Communications Committee (ECC) of CEPT considers and develops policies and non-binding regulations on electronic communications activities for Europe, taking account of European and international legislations and regulations. ECC is the key space for information, harmonisation, and management of radio spectrum use[50] in Europe.

The ECC, in particular on request of its members, undertakes compatibility studies and establishes conditions and parameters under which the sharing between the different users of the spectrum may take place. This may result in the development of an ECC Decision. ECC also develops CEPT Reports when mandated by the European Commission.

A Memorandum of Understanding (MoU) has been agreed between ETSI and the CEPT Electronic Communications Committee (ECC),[51] for co-operation. European Harmonised Standards for radio equipment as well as other relevant ECC deliverables will involve collaboration between ETSI and CEPT.

CEPT/ECC operates through three principal working groups on frequency management, spectrum engineering and regulatory affairs. For many IoT developments, the most important are the frequency management (WGFM) and its subsidiary group SRDMG (Short Range Devices Maintenance Group).[52]

3.8 ETSI

ETSI, the European Telecommunications Standards Institute was created under the auspices of CEPT, which transferred all of its telecommunication standardisation activities to ETSI. ETSI is an independent, not-for-profit association with more than 750 members (including national administrations, companies, and international organisations) beyond Europe. It is one of the official ESOs and also the mirror body to ITU-T.

ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, broadcast and Internet technologies. ETSI has driven the standards for earlier GSM in mobile phones, DECT for cordless phones and now widely used for many IoT applications, or Smart Cards.

ETSI's Harmonised European Standards developed in support of the RED are the preferred means for manufacturers to comply with the regulation. Equipment which complies with the relevant Harmonised Standards is presumed to comply with the requirements of the Radio Directive. As radio equipment also needs to be compliant with electro-magnetic aspects, CENELEC is also involved. ETSI has developed around 350 standards relevant to the RED.[53]

In addition to RED and the multitude of other telecoms standards, ETSI has many standards specifically relevant to IoT development,[54] with an extensive workstream around smart appliances Their current IoT focus is the OneM2M service layer and standard discussed in the previous section – ETSI was one of the founding partners – and which they also promote at the ITU-T. ETSI has also produced a very detail gap analysis for IoT standards.[55]

Work to produce standards is carried out in TGs (Task Groups) consisting of ETSI members from administrations and industry. Many of these will be relevant to IoT, e.g. TG11 (Wideband devices), TG17 (Wireless Microphones and Audio), TG28 (Generic SRDs), TG30 (Ultra Low Power Medical Devices).

3.9 CEN/CENELEC

The European Committee for Standardisation[56] (CEN) and the European Committee for Electrotechnical Standardisation[57] (CENELEC) are the standards organisations for electromagnetic systems. Together with ETSI they are the officially recognised European Standardisation Organisations, with their standards referenced in EU legislation.

Since 2010, CEN and CENELEC operate under a common CEN-CENELEC Management Centre (CCMC) in Brussels. CEN works closely with ISO and CENELEC with IEC in developing standards.

The organisations maintain a large number of critical standards for the safety of European consumers. Only in relation to household appliances, CENELEC maintains over 100 standards,[58] including the regulation of plugs and sockets.[59]

These organisations develop specific standards on demand from the European Commission. Currently, there has not been such a request for IoT, although they are carrying work on smart cities, smart homes, e-health, smart grids and meters, and have many relevant standards, including those related to RFID.[60]

[21] ITU. (n.d.). Terms of Reference. Internet of Things Global Standards Initiative (IoT-GSI) . Retrieved November 27, 2017, from https://www.itu.int/en/ITU-T/gsi/iot/Documents/tor-iot-gsi.pdf

[22] ITU. (n.d.). ITU-T work programme. 2017-2020: SG20. Retrieved November 27, 2017, from http://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=20

[23] ITU-T. (2015). Recommendation G.9959: Short range narrow-band digital radiocommunication transceivers – PHY, MAC, SAR and LLC layer specifications. Retrieved November 27, 2017, from https://www.itu.int/rec/T-REC-G.9959-201501-I/en

[24] Z-Wave Alliance. (2014). Z-Wave Alliance Recommendation ZAD12837-1 – Z-Wave Transceivers – Specification of Spectrum Related Components. Retrieved November 27, 2017, from https://z-wavealliance.org/wp-content/uploads/2015/02/ZAD12837-1.pdf

[25] ISO. (n.d.). Standards Catalogue ISO/IEC JTC 1/SC 41 – Internet of Things and related technologies. Retrieved November 27, 2017, from https://www.iso.org/committee/6483279/x/catalogue/p/1/u/0/w/0/d/0

[26] ISO. (2016). ISO/IEC CD 30141:20160910(E). Information technology – Internet of Things Reference Architecture. Retrieved November 27, 2017, from https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf

[27] IEC. (n.d.). IEC – About the IEC. Retrieved November 27, 2017, from http://www.iec.ch/about/?ref=menu

[28] ISO. (2008). ISO/IEC 18000-1:2008 – *Information technology -- Radio frequency identification for item management -- Part 1: Reference architecture and definition of parameters to be standardized*. iso.org.

[29] BSI. (2016). PAS 212:2016 *Automatic resource discovery for the Internet of Things. Specification.* shop.bsigroup.com.

[30] Hypercat. (2016). *Hypercat 3.00 Specification.* hypercat.io

[31] IEEE. (n.d.). IEEE About IEEE. Retrieved November 27, 2017, from https://www.ieee.org/about/about_index.html

[32] IEEE. (2015). IEEE SA – 2413 – *Standard for an Architectural Framework for the Internet of Things (IoT)*. standards.ieee.org.

[33] IEEE. (n.d.). Internet of Things Related Standards in Development. Retrieved November 27, 2017, from http://standards.ieee.org/innovate/iot/projects.html

[34] IETF. (n.d.). About the IETF. Retrieved November 27, 2017, from https://www.ietf.org/about/

[35] Keränen, A., & Bormann, C. (2016). Internet of Things: Standards and Guidance from the IETF. *IETF Journal.*

[36] Zigbee Alliance. (n.d.). Zigbee IP and 920IP. Retrieved November 27, 2017, from http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeeip/

[37] Shelby, Z., Hartke, K., & Bormann, C. (2014). IETF RFC 7252: *The Constrained Application Protocol (CoAP)*.

[38] Stansberry, J. (2015, October 7). MQTT and CoAP: Underlying Protocols for the IoT. Retrieved November 27, 2017, from http://www.electronicdesign.com/iot/mqtt-and-coap-underlying-protocols-iot

[39] OASIS. (2014). *MQTT Version 3.1.1*. mqtt.org.

[40] Piper, A. (n.d.). *IBM Podcast.* Retrieved from https://www.ibm.com/podcasts/software/websphere/connectivity/piper_diaz_nipper_mq_tt_11182011.pdf

[41] OASIS. (n.d.). OASIS MQTT Internet of Things Standard Now Approved by ISO/IEC JTC1 | OASIS. oasis-open.org.

[42] W3C. (n.d.). W3C Web of Things Working Group. Retrieved November 27, 2017, from https://www.w3.org/WoT/WG/

[43] W3C Begins Standards Work on Web of Things to Reduce IoT Fragmentation | W3C News. (2017, February 24). w3.org.

[44] 3GPP. (n.d.). 3GPP. Retrieved November 27, 2017, from http://www.3gpp.org/

[45] GSMA. (n.d.). GSMA IoT Security Guidelines | Internet of Things. Retrieved November 27, 2017, from https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

[46] GSMA. (n.d.). GSMA Documents. Retrieved November 27, 2017, from https://www.gsma.com/newsroom/gsmadocuments/

[47] GSMA. (2013). *Embedded SIM Remote Provisioning Architecture Version 1.1*

[48] GSMA. (n.d.). GSMA Mobile IoT Initiatives | Licensed Low Power Wide Area Technology. Retrieved November 27, 2017, from https://www.gsma.com/iot/mobile-iot-initiative/

[49] CEPT. (n.d.). About CEPT. Retrieved November 28, 2017, from https://cept.org/cept/

[50] CEPT. (n.d.). ECC. Retrieved November 28, 2017, from https://cept.org/ecc/

[51] CEPT. (n.d.). ECC and ETSI. Retrieved November 28, 2017, from https://cept.org/ecc/ecc-and-etsi

[52] LPRA. (n.d.). European Standards, Regulations and Law » Low Power Radio Association. Retrieved November 28, 2017, from http://lpra.org/resources/european-standards-regulations-and-law/

[53] ETSI. (n.d.). Work Item Plan: All Active Work Items For Directive ‘2014/53/EU’. Retrieved November 28, 2017, from http://bit.ly/2u1oiy2

[54] ETSI. (n.d.). Internet of Things.

[55] ETSI. (n.d.). TR 103 376 – V1.1.1 – *SmartM2M; IoT LSP use cases and standards gaps.* etsi.org.

[56] CEN. (n.d.). Who we are. Retrieved November 28, 2017, from https://www.cen.eu/about/Pages/default.aspx

[57] CENELEC. (n.d.). CENELEC – About CENELEC – Who we are. Retrieved November 28, 2017, from https://www.cenelec.eu/aboutcenelec/whoweare/

[58] CENELEC. (n.d.). Household appliances. Retrieved November 28, 2017, from https://www.cenelec.eu/aboutcenelec/whatwedo/technologysectors/householdappliances.html

[59] CENELEC. (n.d.). Plugs and socket outlets types in each CENELEC country. Retrieved November 28, 2017, from ftp://ftp.cencenelec.eu/CENELEC/TCs/61/PlugsSockets.pdf

[60] European Commission Standardisation mandate in the field of information and communication technologies applied to radio frequency identification (rfid) and systems M 346 2008

4. Standards for IoT

Interoperability is an important issue in a new technology where regulation is not completely settled, as developers face decisions where the consequences are difficult to evaluate. Investing time and money in a particular technology only to see it disappear, become irrelevant, or simply incompatible with most other offers in the sector is a real risk. Lack of interoperability forces developers who want to reach across systems to build the compatibility in their products, through extra components that can interface with various systems, thus increasing complexity and costs.[61]

Standards are a major form of industrial regulation driving interoperability and critical for modern industrial organisation. The argument against standardisation is that similarly to excessive regulation it can discourage innovation and protect incumbents against newcomers. The OECD has raised serious concerns about the interoperability of technologies but also warns against imposing inflexible standards.[62] A fine balance must be found. The relationship between regulation and standards is complex and beyond the scope of this report.

The very concept of an *Internet of Things*, contains a core principle of interoperability, as this is the basis of the Internet itself: computers being able to talk to each other by using open shared protocols that are agnostic to the content distributed at that level or where it comes from. However, the reality is that many networks created in industrial contexts, or for home automation, were not designed to be connected to the wider world.

Interoperability in IoT could mean very different aspects depending on the level: basic physical compatibility of radio spectrum and electrical systems, discoverability and interactions among devices, data flows for reuse or applications working with each other.

There is a certain fragmentation of standards in IoT, but there is also a lot of complexity and separate layers, so many of those standards do not necessarily compete directly with each other. There is a difference between intergovernmental organisations, such as ITU, standards bodies – ETSI, IEEE or IETF – and industry consortia formed around a common protocol vying for dominance in a sector – as is the case of Thread, Zigbee or Z-wave. Not all companies engage in all out competition, however, with many companies such as Cisco or Samsung supporting competing standards. Other companies such as Google promote their own standard with a view to expand their offer from other areas. Some standards are formed by complex consortia of standard bodies and industry, and industry populate standards bodies, but in theory they are neutral and do not promote a particular interest. Industry associations such as GSMA will promote technological paths – such as GSM mobile radio vs free spectrum – but not a single business.

There are many separate industrial areas under the umbrella term IoT. Cars, health or energy have very different needs and will have separate regulations and standards, as in most cases interoperability will not be an issue, say for example between cars and hospital equipment. There are, nevertheless, efforts to build common frameworks between the infrastructure level and the applications, such as oneM2M. IoT at home or in wearables is generally more driven to standards than industrial automation as individual consumers cannot usually negotiate interoperability after the purchase of a specific technology in the way a hospital or a municipality might do. Standards can be specific to IoT, or general communication standards applied to IoT, such as wifi or Bluetooth. This report focuses on the former.

Intellectual property is a critical aspect of standard for developers, particularly around the use of patents. Most IoT standards and protocols are available on a royalty-free basis and many in a full open source version completely unencumbered by patents, which seems a dominant theme. Many standards also have a certification regime, although the majority will not restrict the use of the standard to certified products.

Subtle differences in the licensing regime can be important and developers should study carefully how these may impact their design processes and business models, which will also have an effect on their data policies and other ethical decisions.

In the EU, certain standards bodies[63] – such as ETSI – are able to create official standards that can be referred to by EU Regulations and Directives – this is obviously important for developers and it is a way in which policymakers can incentivise the creation and use of specific technical standards and avoid monopolistic tendencies. These standards are discussed in the sections about telecoms and electrical regulation.

Below is a non-exhaustive overview of the main standards and related organisations specific to IoT.

4.1 The OSI Layers Model

In order to understand the regulation and standardisation of the Internet of Things landscape it is useful to map the various efforts, organisations, and protocols to some established conceptual models for networks, used to define most networking technologies for the past 30 years.

The Open Systems Interconnection[64] (OSI) model was adopted by the International Standards Organisation, as standard ISO 7498, in the mid 1980s as an international effort to bring an end to the closed monopolies that companies such as IBM had been developing in the postwar decades.[65] The OSI model never reached commercial success as a fully formed technology and was superseded by the US-led Internet. However, the conceptual OSI model around layers remains useful in contemporary contexts, although with some limitations as we will see below. Here we will give a very brief overview of the model.

The OSI model defines seven layers that sit on top of each other providing levels of abstraction that ideally allow each layer to operate without having to worry about the internal workings of the levels below. Each layer would have its own protocols, although some of the IoT protocols discusses in this section will cover more than one layer. For the purposes of this paper it is not necessary to be too strict, as the objective of introducing the OSI model is to enable understandings of the interrelations between regulations, standards and protocols that IoT developers may have to navigate, and not to provide an authoritative taxonomy.

One important distinction is between the upper and lower layers of the OSI model. Upper layers are the aspects of networking that many technology users will encounter and recognise in more direct form and operate with *data*. Lower layers typically operate either within the internals of machines or at the infrastructure level and deal with raw information in *bits, frames and packets* among other. Working from top to bottom:

Upper layers:

1. Layer 7 – *Application*. Deals with supporting applications, and would include things such as the http protocol for web access and the smtp protocol for sending emails. Some specific IoT application layer protocols for sending data across low bandwidth devices include the lightweight MQ Telemetry Transport Protocol[66] (MQTT) and the web-based Constrained Application Protocol (CoAP).[67]
2. Layer 6 – *Presentation*. Converts data into a useful form for applications, covering for example XML data structures or compression. Importantly for discussions around privacy it is where encryption typically takes place, although this is not always the case. The IETF RFC 1085 standards aka Lightweight Presentation protocol (LPP) is a common IoT protocol for this layer.

- For practical purposes layers 6 and 7 are merged in many modern systems.
- Layer 5 – *Session*. Will handle specific exchanges of data. Internet phone calls for example will use some session protocols to start and end.

Lower layers:

- Layer 4 – *Transport.* This layer is where a lot of the sending of information online occurs, with segmented chunks of information travelling back and forth. These protocols ensure, for example, that an email or image arrives complete to its destination.
- Layer 3 – *Network*. This layer defines modern communications with the concept of packets of information that can be sent to its destination via different routes. *The Internet Protocol (IP)* sits here, ensuring that messages find their way to receivers and requests for websites reach the servers holding the information. The Zigbee IoT standard defines its own non-internet protocol in this layer.[68]

The two bottom layers deal with physical infrastructure and can be bundled together in many systems:

- Layer 2 – Data link. This layer ensures that devices can talk to each other and that basic information broken into tiny parts arrives without errors. Bluetooth, cable ethernet or the ubiquitous wifi are some of the best known examples here. The IEEE 802.15.4 standard for low-rate wireless personal area networks (LR-WPANs) is one of the key IoT protocols at this level, and provides the basis for several standards including Zigbee, 6LoWPAN and Thread. Other IoT protocols in this layer include Z-Wave and various proprietary standards for devices such as garage door openers.
- Layer 1 – Physical. This involves sending digital ones and zeros in the form of electric signals or wavelengths across copper, fibre optic, or radios.

The OSI model is not the only way to conceptualise networking. For example, the Postscapes project provides a non-layered classification of IoT protocols based on functional characteristics – e.g. infrastructure, identification, device management, discovery, semantic.[69]

[61] Sharron, S. L., & Tuckett, N. A. (2016, February 2). The Internet of Things: Interoperability, Industry Standards & Related IP Licensing Approaches. Retrieved November 27, 2017, from https://www.sociallyawareblog.com/2016/02/02/the-internet-of-things-evaluating-the-interplay-of-interoperability-industry-standards-and-related-ip-licensing-approaches/

[62] OECD. (n.d.). *DSTI/ICCP/CISP(2015)3/FINAL – The Internet of Things: Seizing the Benefits and Addressing the Challenges.* oecd.org.

[63] European Commission. (n.d.). European Standards – Growth – European Commission. Retrieved November 27, 2017, from https://ec.europa.eu/growth/single-market/european-standards_en

[64] Zimmerman, H. (1980). OSI Reference Model--The ISO Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications*, 28(4), 425–432. http://doi.org/10.1109/TCOM.1980.1094702

[65] Russell, A. L. (2014). Open Standards and the Digital Age. Cambridge University Press.

[66] OASIS. (2014). MQTT Version 3.1.1 . Retrieved November 27, 2017, from http://mqtt.org/

[67] Bormann, C. (n.d.). CoAP — Constrained Application Protocol | Overview. Retrieved November 27, 2017, from http://coap.technology/

[68] Frenzel, L. (2013, March 22). What's The Difference Between IEEE 802.15.4 And ZigBee Wireless? Retrieved November 27, 2017, from http://www.electronicdesign.com/what-s-difference-between/what-s-difference-between-ieee-802154-and-zigbee-wireless

[69] Postscapes. (n.d.). IoT Standards & Protocols Guide | 2017 Comparisons on Network, Wireless Comms, Security, Industrial. Retrieved November 27, 2017, from https://www.postscapes.com/internet-of-things-protocols/

5. Current IoT-Specific Standardisation Efforts

The organisations and projects described in this section are a small subset of all the projects developing standards. Most of these are industry-led consortia, with various degrees of collaboration with standards organisations and other stakeholders. Most of these technologies are not fully formed standards, but industry agreed protocols and designs. They tend to be based on standards created by the organisations discussed in the previous section.

In some cases, such as Z-Wave or Hypercat, these industry standards are then taken to standards bodies to be adopted more widely. It is unclear what practical impact making these technologies official standards have on their adoption, or whether this is primarily about gaining symbolic legitimacy.

The fully formed commercially available home automation technologies discussed below – Thread, Zigbee, Z-Wave and Bluetooth – remain fragmented, but at another level there has been convergence on the Open Connectivity Foundation and the oneM2M standard for industrial settings. At the moment, these technologies are one level removed from end users, and it is unclear whether they will form their own branded consumer framework or interoperate with other technologies. It is also worth mentioning that the WIFI alliance is working on a low energy specification called HaLow for smart home and IoT devices.[70]

The initiatives here show a convergence of technologies toward the internet and web, and also the importance of an open source model, with almost all the projects having at least some of its technology available as open source.

Another important aspect is the certification of devices and applications. Almost all the initiatives have a certification programme, with some such as Z-Wave requiring this in order to brand the products.

The projects covered here mainly involve the connection of devices, and these choices would be the main decisions developers will be encountering in their designs.

5.1 OneM2M

The OneM2M group[71] brings together over 200 manufacturers, telecoms service providers and regional standards bodies from North America, Europe and East Asia. ETSI is heavily involved from Europe, and by extension the ITU.

The focus of oneM2M is developing a "service layer", which sits between the mid-level layers of "network" of hardware or basic software that provide data transport and the top layers of "applications" that generate or use the data. It is mainly expected to ride on top of the internet protocol. The aim is to enable access to functions commonly needed by actions across various industries – discovery, device management, subscription or billing – in what is called horizontal interoperability.[72]

Their work includes a suite of standards for machine-to-machine and other IoT applications, including a set of security solutions.[73]

This standard is more relevant to developers working toward smart city or business applications (transport, health, energy, etc.), but if it becomes successful it may expand to other uses. The standard also highlights the different approaches between top down industry efforts and independent developers.

5.2 Open Connectivity Foundation

The Intel driven Open Connectivity Foundation (OCF) is backed by over 300 companies, including the manufacturers of many of the chips found in most consumer computing devices, such as Qualcomm and Atmel – and many industry heavyweights: Cisco, General Electric, Microsoft, Dell, Intel and Samsung, among others. The OCF has merged in the Allseen Alliance initially driven by Qualcomm and run by the Linux Foundation, which had developed the AllJoyn open source IoT framework.

The consortium is developing a framework for the discovery and secure interoperability of devices running multiple operating systems, platforms, modes of communication, transports and use cases. The group makes available their framework in an open source implementation called Iotivity[74] and have a certification programme. Like most other organisations in the sector they have a strong interest in security.

The Iotivity framework works at the higher layers of the OSI model. Like oneM2M, it also describes itself as providing a "service layer"[75] that allows devices to work together. The project uses the CoAP protocol for sending data around and has plugins to interoperate with various technologies such as Zigbee and Bluetooth Low Energy.

This project is a lot more relevant to independent developers, with its open source approach and implementation in a variety of consumer and mobile platforms. The involvement of the Linux Foundation could allow a wider range of stakeholders to be involved in the development of the technology, despite the important role of industry. This could have long term implications for how any ethical issues arising with the technology might be dealt with. Participation from independent developers and organisations not driven by profit might allow for a better consideration of ethical issues.

Industrial Internet Consortium

The Industrial Internet Consortium[76] includes some of the largest companies developing IoT technologies, such as AT&T, Cisco, General Electric, IBM, and Intel. The Industrial Internet Consortium is managed by the Object Management Group (OMG). The IIC has been mainly developing testbeds for approximating real life applications of industrial IoT.

The OMG is not exactly a standard setting organisation. They build reference architectures and models mainly at the process or language level, which may then get incorporated as standards by other organisations such as ISO. One example is the Unified Modelling Language (UML).[77] Their work on IoT standardisation appears to be at a fairly early stage, no doubt due to the need to work in separate areas such as transport, health or energy.

This project is not relevant to developers in the short terms, but similarly to the oneM2M standard, it may well become more relevant as the technology is developed and implemented more widely.

5.3 IPSO Alliance

The IPSO Alliance[78] is formed from a large network of industrial and technology companies, including Bosch, Arm, Intel, Ericsson, and Google. Their work covers discoverability and identification based on semantics, and security and privacy based on identity.

IPSO is not a standards organisation, it promotes and supports common data structures to define Smart Objects, and manages an IPSO Smart Object Registry that includes libraries, icons and repositories to be used by standards organisations and other communities or independent developers.

IPSO has the goal of creating other useful components definitions, instantiations, data models, design models, reference architectures and icons – all of which are open – for objects such as smart washing machines, fridges, barometers, etc. From a traditional networking perspective this happens at a very high level, and the IPSO systems interoperate with various application layer protocols.

The work of IPSO is based on promoting the use of the IP protocol for Smart Objects, which is a critical development for a true *Internet of Thing*s, and the use of web technologies.[79] IPSO has worked with the standards bodies discussed in the previous sections and also with the Zigbee project,[80] which has since expanded their technology to IPv6.

5.4 Open Mobile Alliance

The Open Mobile Alliance (OMA)[81] was formed by the mobile industry to promote interoperability with a focus on IoT. The OMA develop standards that work at fairly high layers and can operate on both cellular networks and other types of infrastructure.

The OMA has developed over 200 specifications and standards, but its better-known work is the LightWeightM2M (LwM2M) specification, currently implemented by over 25 companies in their IoT platforms, including Huawei's OceanConnect and ARM mbed.

LwM2M is a device management protocol designed for remote management and services of low power devices and sensor networks. It is based on modern web standards such as REST, and transfers data through the Constrained Application Protocol (CoAP). LwM2M is based on protocol and security standards from the IETF,[82] and also includes IPSO's objects.

The specification is freely available and there is an open source toolkit. The OMA has a clear outreach to developers.

5.5 Long Range Networking

Most home and consumer devices connect to a base station of some form, normally either a mobile phone or home router, which then provides a wide-area connection to another system and eventually the internet.

Low Power Wide Area (LPWA) technologies provide direct connectivity to broader systems over long distances of over a kilometre. This could involve a smart city, agriculture, energy or many other systems. Although until now these technologies have been mainly driven by industry there is growing interest from citizens and communities, for applications such as bike sharing.[83]

In many cases these devices are designed to operate on batteries unsupervised for a long time – 10 to 20 years – which may raise issues of spectrum and electronic pollution on the future. These systems are also designed to handle hundreds or thousands of connected devices.

The two main technical approaches have been to either lower the power consumption of mobile telephony technologies and to extend the range of low power home networks.[84] There is growing standardisation in this sector[85] although closed proprietary systems are still popular. Below we give an overview of some of the main initiatives.

5.6 Sigfox

Sigfox is a French company that has developed a proprietary system with a range between 3 and 50 km and uses free spectrum without the need to acquire licenses. Sigfox devices are designed to handle low data-transfer speeds and consume only 50 microwatts compared to 5000 microwatts for mobile data,[86] and have a typical stand-by time 20 years with a small battery. There are deployments of Sigfox in various cities.

This technology is perhaps not very relevant for many independent developers, but it offers an idea of the kind of successful commercial applications available. In addition, developers wishing to build devices or tools for cities where Sigfox is in operation may need to work with them through their partner network.[87]

5.7 Lorawan

The Lorawan Alliance develops a system also based on free industrial, scientific and medical (ISM) radio bands, with low power requirements and similar range to Sigfox. It has been deployed in over 150 cities and the alliance has over 400 members.[88] The alliance provides a certification programme for its members.[89] The technology is based on closed intellectual property, but it is available for implementation.

Lorawan is the main technology supported by The Things Network,[90] which is an open source, decentralised global infrastructure for the Internet of Things, with a community edition free for fair use. The Things provide community groups with local gateways and pooling of resources allowing the development of applications, and for device owners to make their data available to a wider community.

5.8 Weightless

Weightless provides a set of standards that cover different applications. Their Weightless-W standards operates on free TV spectrum and it is geared to industrial operations, their Weightless-N standard is geared for sensors networks and is similar to Sigfox.

Weighless-P is their newest LPWAN standard for more general use and aims to compete with the solutions based on mobile phone technology[91] in terms of performance, network reliability and security.

Weightless are sophisticated technologies and a fully open standard unencumbered by patents or other IP restrictions. As such, it may be interesting for ethical developers, who may want to be able to enable an open source approach to their designs – allowing others to freely build on them to develop their own designs – with absolute certainty that they will not encounter problems. The Weightless alliance however charge a developer fee to cover costs. The deployment of the technology in the field is not as widespread as Sigfox or Lorawan.

5.9 Cellular Standards

3GPP has developed a set of standards for IOT, which include includes NB-IOT, eMTC and EC-GSM-IoT.[92]

These technologies are mainly based on software upgrades to existing mobile telephony infrastructure and therefore expect to have lower introductory costs as there is no need to build new antennas our repeaters. These technologies aim to deliver similar range, efficiency, and range as the technologies based on LPWAN discussed above, but with more data bandwidth in some cases.

These developments pave the way for the implementation of 5G next generation mobile technology. This promises a major revolution in terms of speed and connectivity, but major issues remain in terms of large investments required and proposals to reserve dedicated capacity for industrial sectors.

5.10 Further reading

- The Low Power Radio Association is a source of information and potential support for IoT developers.[93]
- Comprehensive information on the regulatory environment is provided by ETSI and CEPT/ECC.[94]
- A case study illustrating how regulations and standards come together in practice is provided by the RFID in Europe association.[95]

[70] Wi-Fi Alliance. (n.d.). Wi-Fi HaLow. Retrieved November 27, 2017, from https://www.wi-fi.org/discover-wi-fi/wi-fi-halow

[71] oneM2M. (2015, January). oneM2M, the interoperability enabler for the entire M2M and IoT ecosystem. Retrieved November 27, 2017, from http://www.onem2m.org/about-onem2m/why-onem2m

[72] Yamasaki, N. N. (2017). oneM2M Standards Activities. Presented at the w3.org. Retrieved from https://www.w3.org/2017/05/wot-f2f/slides/20170516-W3C-oneM2M.pdf

[73] oneM2M. (2014). *TS-0003-Security_Solutions-V-2014-08.doc.* onem2m.org

[74] IoTivity. (n.d.). Home | IoTivity. Retrieved November 27, 2017, from https://www.iotivity.org/

[75] IoTivity. (n.d.). IoTivitiy Architecture. Retrieved November 27, 2017, from https://wiki.iotivity.org/architecture

[76] Industrial Internet Consortium. (n.d.). Industrial Internet Consortium. Retrieved November 27, 2017, from http://www.iiconsortium.org/

[77] ISO. (n.d.). *ISO/IEC 19505-1:2012 – Information technology -- Object Management Group Unified Modeling Language (OMG UML) -- Part 1: Infrastructure.* iso.org.

[78] IPSO Alliance. (2016, August 11). Enabling IoT Devices' Hardware and Software Interoperability. Retrieved November 27, 2017, from http://www.ipso-alliance.org/wp-content/uploads/2016/11/2016-11-08_IPSO_Overview.pdf

[79] Jimenez, J. (2015). An Introduction to IPSO Smart Objects. Retrieved November 27, 2017, from http://iot-week.eu/wp-content/uploads/2015/06/03-IPSO_Introduction.pdf

[80] Wikipedia. (n.d.). IPSO Alliance – Wikipedia. Retrieved November 27, 2017, from https://en.wikipedia.org/wiki/IPSO_Alliance

[81] Open Mobile Alliance. (n.d.). Open Mobile Alliance Mobile Phone Standards & Specifications. Retrieved November 27, 2017, from http://openmobilealliance.org/

[82] Open Mobile Alliance, open. (n.d.). Lightweight M2M (LwM2M). Retrieved November 27, 2017, from http://openmobilealliance.org/iot/lightweight-m2m-lwm2m

[83] Vulic, L. (2016, February 29). A bicycle tracking system in Budapest on a LoraWan network – MikroElektronika. Retrieved November 27, 2017, from https://www.mikroe.com/a-bicycle-tracking-system-in-budapest-on-a-lorawan-network/

[84] Low-Power Wide-Area Networks at the IETF. (2016, November). Low-Power Wide-Area Networks at the IETF. Retrieved November 27, 2017, from https://www.ietfjournal.org/low-power-wide-area-networks-at-the-ietf/

[85] Winchcomb, T., Massey, S., & Beastall, P. (2017). Review of latest developments in the Internet of Things. Cambridge Consultants

[86] RS Components. (n.d.). 11 Internet of Things (IoT) Protocols You Need to Know About. Retrieved November 27, 2017, from https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

[87] Sigfox. (n.d.). Sigfox Partner Network. Retrieved November 27, 2017, from https://partners.sigfox.com

[88] LoRa-Alliance.org. (n.d.). LoRa™ Alliance Overview. Retrieved November 27, 2017, from https://docs.wixstatic.com/ugd/eccc1a_de5fda268ed945e885a43a39b387528d.pdf

[89] LoRa-Alliance.org. (n.d.). LoRa Alliance™ Certification Overview. Retrieved November 27, 2017, from https://www.lora-alliance.org/certification-overview

[90] The Things Network. (n.d.). The Things Network. Retrieved November 27, 2017, from https://www.thethingsnetwork.org

[91] Weightless Management Ltd. (n.d.). New LPWAN open standard reinvents IoT. Retrieved November 27, 2017, from http://www.weightless.org/about/new-lpwan-open-standard-reinvents-iot

[92] 3GPP. (2016, June 22). Standardization of NB-IOT completed. 3gpp.org.

[93] LPRA. (n.d.). Low Power Radio Association. Retrieved November 28, 2017, from http://lpra.org/

[94] ETSI, CEPT/ECC. (2016). *The European regulatory environment for radio equipment and spectrum: an introduction*. etsi.org.

[95] Standards & Regulations | RFID in Europe. (n.d.). Retrieved November 28, 2017, from http://www.rfidineurope.eu/sr

6. Technical Regulation

The regulation of telecommunications and electrical equipment in Europe is a complex field with a direct impact on IoT developers, who must ensure that any devices comply with various regulations and standards.

This section offers an overview of the main legislation, under the Telecommunications Framework, with the caveat that it is under review, and the New Legislative Framework for product, which covers regulations of radio equipment and electrical devices. This section also describes the main organisations driving policy and how they work together. Finally, key regulatory issues for IoT in regards to telecommunications are outlined.

6.1 Regulatory Framework

Telecoms Package

The European "Telecoms Package" provides the basis for regulation in this area. It is composed of several directives and its current form was started in 2002, although it is currently under review.

The Framework Directive'[96] sets out the main rules. The stated principles of the directive are to strengthen competition in the electronic communications sector, stimulate investment, and foster freedom of choice for consumers.

The Telecoms Package includes four 'specific' Directives which regulate various aspects of electronic communications, as well as two Regulations:

- Directive 2002/20/EC or 'Authorisation Directive'[97] covers authorisations for all electronic communications networks and services, whether they are provided to the public or not. It applies to the granting of rights to use radio frequencies where such use involves the provision of an electronic communications network or service, normally for remuneration.
- Directive 2002/19/EC or 'Access Directive'[98] harmonises the way in which EU countries regulate access to, and interconnection of, electronic communications networks and associated facilities. It establishes a series of principles to ensure access and interoperability: transparency, non-discrimination, etc; some price controls.
- Directive 2002/22/EC or 'Universal Service Directive'[99] forces telecoms providers to provide minimum services and serve people with disabilities or low incomes with specific support. This could be relevant to developers designing specific services or devices for such constituencies or those targeting rural and remote areas.
- Directive 2002/58/EC or 'E-Privacy Directive'[100] establishes rules on confidentiality, electronic marketing and various other aspects. It is relevant for IoT developers as it restricts operators from being able to reuse subscriber data. This Directive is currently being replaced with a regulation, and will be discussed in more detail below.
- Regulation (EC) No 1211/2009 establishing a Body of European Regulators for Electronic Communications (BEREC).[101]
- Regulation (EU) No 531/2012 on roaming on public mobile communications networks[102] has some impact on IoT developers, and a huge impact on citizens who travel within the EU, but it is not clear whether it covers IoT devices. This issue is discussed in the next sections.

Telecoms Review

Infrastructure Competition VS Access and Price Control

The Telecoms framework is under review and industry lobbies are targeting various aspects. The major telecoms industry body, ETNO, wants to move away from the promotion of access-based and price control competition, claiming this "has often undermined the investment incentives of both new entrants and incumbent operators".[103]

They promote instead the concept of "infrastructure competition"[104] with different types of access to the network. Access in this view was useful for solving the problem faced when opening up legacy national telecom monopolies, but nowadays it would be healthier to promote diverse technologies, say cable vs ADSL. Regulation forcing access to buildings and roads to build infrastructure would in this view be more effective than forcing incumbents to open up their networks to potential competitors.

The direction of these reforms will matter for IoT developers, as a move to infrastructure competition could force major investments in networking and wireless. Many EU countries already have a very diverse infrastructure landscape.

6.2 The European Electronic Communications Code

In September 2016, as part of the new "Connectivity Package"[105] the European Commission published its proposal for a directive establishing the European Electronic Communications Code.[106] This is important for IoT developers, as it could determine the exact regulation covering their devices and services.

The Code re-establishes the definitions of Electronic Communication Services (ECS), which are now subdivided into 1) Internet Access Services (IAS), 2) Interpersonal communications services, which can be of two types: number-based such as phone calls or Skype, and number-independent. For these there must be at least one natural person involved and the recipients must be taken from a finite number of recipients chosen by the sender, and excludes broadcast-style services. There is some confusion as to where social media would fall in this classification. The third category would be 3) services consisting wholly or mainly in the conveyance of signals, such as machine-to-machine and broadcasting.

Currently, Skype, Whatsapp, and other internet services are not covered by most Telecoms regulations, like landline phone or mobile calls of texts are, and the new classification aims to partially close this gap.

There is a debate about how IoT services should fit in the classification. The Code seems clear on having a separate pure machine-to-machine category, which may cover industrial or smart city IoT, many IoT devices and services will interact with people, though, and blur those lines. Industry seeks to reduce the regulation on IoT devices by classing them separately from communications services.

ETNO believes that IoT services should be considered outside the scope of the definition of communication services provided to end-users: "communications with and between machines substantially differ from traditional communication between individuals and the regulation in this framework and the regulation applicable to communication services would not be relevant nor fit for purpose for M2M/IoT related services."[107]

GSMA believes that "careful consideration should be given to Internet of Things (IoT) services provisioning. Many IoT services will be available to consumers in the future, from connected fridges to pet trackers, burglar alarms to connected cars, which may include some element of connectivity without being either an internet access service or interpersonal communications service. The GSMA recommends restricting sector-specific end-user protections to internet access services and interpersonal communications services, and to apply conveyance of signals sector-specific regulation only to requirements relating to security and privacy."[108]

From the point of view of privacy and consumer protection it is better if IoT devices are covered by communications rules and not just as signals conveyance.

6.3 E-Privacy

The regulation of e-privacy is one of the aspects of the Telecoms Package that has a large impact on IoT developers. While many other aspects of telecoms regulation will affect the operators of networks or large systems, the new E-Privacy regulation[109] (E-pR), currently being approved by the EU, will place obligations on device manufactures and app developers. The regulation is still being amended, but it will certainly put new privacy protections in place for personal IoT devices.

The previous version of this law was popularly known as the Cookie Directive, as it is the origin of the infamous banners that appear on most websites. The new version aims to improve this situation among other reforms. The instrument is much broader than cookies, covering online marketing, security, restrictions for telecoms companies to access and reuse subscriber data and a ban on monitoring their communications.

The new E-pR works in tandem with the GDPR to protect the confidentiality of communications and the broader privacy of users. The e-privacy Regulation is broader, covering also "non-personal" data. For example, this is important if sensor data is transmitted without attached identifiers, which under GDPR may not be classed as personal, but must still be confidential under E-Privacy.

IoT developers will need to be particularly aware of the restrictions on devices and the principle of confidentiality of communications, which means developers cannot simply reuse data generated by users without consent. The E-pR also sets out some rules on the tracking of devices form their signals, typically seen in wifi tracking in shopping malls, and with street furniture.

Recital 12 explicitly states that the Regulation is designed to cover the Internet of Things. However, while it is fairly clear that this includes portable devices and smart home appliances, it is unclear whether some industrial or smart city settings would be covered. Its application to wearable sensors is also unclear, with doubts about how to treat raw data in the framework set out in E-pR.[110]

6.4 Net Neutrality

Net neutrality is based on the principle of "best effort", meaning that telecoms operators should give equal treatment to all types of data traffic being transmitted over the internet. Best efforts should be made to carry data without looking at content and being agnostic to the applications involved. This is based on the separation between application and network layers in the OSI model. This separation is supposed to enable innovation of applications independent of the ISP and help support end-user choice.[111] Net neutrality does not generally cover control of traffic for security or technical improvements.

Net neutrality problems could involve ISPs restricting peer-to-peer file sharing other than to prevent actual bottlenecks, or mobile companies providing free data for specific services such as Netflix or Spotify out a data plan.

In Europe net neutrality is codified in law through the long-winded Regulation 2015/2120 *laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.*[112]

The Regulation provides various measures for an open internet along the lines described above. The application of net neutrality in practice is quite complex, with regulators apparently reluctant to stop services without strong evidence of market distortions.[113] The European regulatory body BEREC provides guidelines for implementation.[114]

Net neutrality is crucial for the flourishing of consumer IoT, despite the fact that strict machine to machine communications are specifically excluded from these rules in Europe.

Concerns about a weakening of these rules in the USA have generated a debate among IoT stakeholders in that country.[115] Internet providers with control over the home hub and router that would connect smart devices to the internet are in a strong position for promoting their own platforms. Speed is of the essence in real time services such as alarms and thermostats, and even small delays through traffic management could have an impact.

6.5 The New Legislative Framework

The New Legislative Framework was adopted in 2008 and came into full force in 2017. This is a "package of measures that aim to improve market surveillance and boost the quality of conformity assessments. It also clarifies the use of CE marking and creates a toolbox of measures for use in product legislation".[116]

The current EU approach to regulating products has moved from establishing detailed top down technical regulations to a more flexible approach that only defines essential requirements in legislation and works the detail through associated harmonised standards, delivered through mandates to the ESOs.

The new framework avoids situations where the responsibility for faults or outright counterfeit products was unclear. The new framework gives responsibilities to every actor on the supply chain, from designers and suppliers to importers and distributors when the product is made available in the EU.[117]

The new approach places the onus on the manufacturers, importers and distributors to prove conformity, but it does not require authorisations before going to market. Instead it creates a responsibility for governments to ensure that products placed in the market are safe through market surveillance. This means that specific authorities must regularly visit commercial spaces and industrial settings obtaining samples and checking products functioning in real life situations. These authorities can require all form of documentation.

The relevant European laws are the Radio Equipment Directive (RED), the Low Voltage Directive (LVD) and the Electromagnetic Compatibility (EMC) Directive. Consumer goods with a voltage below 50 V for alternating current or 75 V for direct current are dealt with by the General Product Safety Directive (GPSD) 2001/95/EC, which are discussed in the following sections.

RED will apply to most IoT devices, as these tend to have some form of radio connectivity. Internet of Things devices that do not have an antenna to transmit or receive radio waves will be covered by the other directive, which also provide a similar set of regulations to ensure that users are safe and the equipment does not cause interference with other products.

The directives are complementary. This means that IoT devices covered by the RED, for example, are not subject to the Low-Voltage Directive (LVD) or the Electromagnetic Compatibility Directive (EMCD). The latter cover wired devices and their prescriptions are similar, so an IoT developer will still have similar obligations either way. The bodies involved in setting the standards are different for each.

In addition to radio and electronic equipment, the framework includes several directives regulating aspects of consumer or industrial safety, such as pyrotechnics, watercraft, civil explosives, measuring instruments, lifts or gas appliances among others. Potentially relevant to some IoT developers are the Toy Safety Directive 2009/48/EU and the planned review of the directive on medical devices.[118]

In the UK, for example, market surveillance authorities include the Health and Safety Executive, the Medicines and Healthcare Products Regulatory Agency and the Trading Standards offices at local authorities. The framework also includes processes for certification and assurance.

6.6 The Blue Guide

The 2016 'Blue Guide'[119] is an official EU document that provides comprehensive guidance on the implementation of European rules for industrial or consumer products, excluding food and agriculture. It covers the directives discussed above but also various other areas such as hazardous substances or industrial machinery. It also covers general product safety and liability. IoT developers wishing to place products in the EU market would benefit from familiarising themselves with this guide.

6.7 Product Directives

Radio Equipment Directive

The Radio Equipment Directive 2014/53/EU[120] (RED) harmonises the laws of the Member States relating to making radio equipment available on the market. Fully applicable since July 2017, the RED defines essential requirements for health and safety, electromagnetic compatibility, and the efficient use of the radio spectrum to avoid interferences. It applies to all products using the radio frequency spectrum, even if for secondary functions such as location positioning, and will include many IoT devices:

> The field of application of this Directive covers a large scope of equipment, ranging from satellite communications to radars, to products operating below 9 kHz such as telecoil hearing aids and sound and TV broadcast receivers. Examples of equipment covered by the guide include combination of multiple radio products in one radio equipment, combination of radio and IT or electro-technical equipment, RLAN enabled domestic appliances, radio controlled heating systems, radio controlled lighting systems, products including GPS, Wi-Fi, Bluetooth, etc.[121]

An important aspect is that the RED applies to equipment that is placed on the market but not to the "relevant components" of radio equipment. This is important for developers of components. Telecom terminal equipment is not covered by RED and falls under other electronics regulation which will be discussed in the next section.

The Directive does not require pre-approval of new equipment, but manufactures or importers must carry out a conformity assessment that will include safety and risks. This must now take into account reasonably foreseeable usage conditions. This means that a manufacturer must consider a potential misuse of the equipment, not just the intended use as outlined in the equipment's instructions. This assessment can reuse safety checks from component suppliers but those assembling the final product are responsible.

The RED allows for self-certification, but also gives the possibility to obtain certification or full quality assurance from a "Notified Body" from a closed list of European technical organisations.[122]

Other obligations include producing various documents, such as traceability, numbering, instructions and safety and technical documentation. Detailed guidance for compliance has been published by the EC.[123]

The RED dos not cover kits used solely for research and development, and this could prove a grey area for IoT developers. In principle, this is aimed at professionals in specialised facilities and not amateur electronics enthusiasts.

Software compliance could prove a difficult area. Software – including updates – that affects the behaviour of the radio operation must be tested for conformity. If the real world operation of devices includes open source software, in principle manufacturers need to test for this possibility. This has raised concerns, particularly among DIY developers who alter wifi routers with open source custom firmware. The Free Software Foundation Europe ran a public campaign labelling the legislation the "Radio Lockdown Directive".[124]

The main concern is that manufacturers faced with requirements to ensure safety with open source will simply lockdown their devices so it is impossible to modify them. Free software advocates ask for exemptions to be made in national legislations or through secondary rules to ensure this does not happen. The actual impact is so far unclear.

6.8 Radio Spectrum Decision

In addition to the RED, another element of radio regulation is the Radio Spectrum Decision (676/2002/EC).[125] This decision coordinates policy within the EU on the availability of radio spectrum and technical conditions for its efficient use. It applies the allocation of radio and wireless communication frequencies for almost every type of IoT device or network.

The decision sets out the roles of the radio Spectrum Committee, the Commission and the relevant standards bodies. This is a very complex and technical policy area, and developers will probably only need to have a simple understanding. We briefly discuss some of the relevant spectrum issues below.

6.9 Low Voltage Directive

The Low Voltage Directive 2014/35/EU (LVD[126]) applies to electrical products with an internal AC current between 50 and 1000 volts. This range covers domestic as well as many industrial applications. From an IoT perspective the LVD could apply to some smart appliances that do not have radio capabilities, but it excludes some small gadgets. The LVD and the EMCD discussed below apply to telecoms terminal equipment

The regulatory principles are similar to those in the RED – market surveillance, conformity, standards – and the Blue Guide applies. The framework has been simplified by making these directives complementary, so that only one applies to a product. This means though that provisions in these directives may overlap. The risk and conformity focus on the LVD is safety, rather than interference.

6.10 Electromagnetic Compatibility Directive

The Electromagnetic Compatibility Directive 2014/30/EU (EMCD)[127] works in tandem with the LVD, but focuses on interference to other equipment and the stability of electrical systems. It also sets out that equipment should have some immunity to electromagnetic radiation.

The EMCD covers fixed installations and not just individual pieces of equipment and therefore could be particularly relevant to some smart city or smart home approaches.

General Product Safety Directive (GPSD)

The General Product Safety Directive (GPSD) 2001/95/EC provides a backstop for any consumer products not covered by any specific legislation.[128] The EU is in the process of replacing the directive with a new regulation that will further harmonise these provisions, but the process is slow.[129]

Its governing principles are similar to the product directives discussed above in relation to market surveillance, but the products under this directive do not require CE marking or a formal declaration of conformity. The products should be safe, however, with self-certification and standards being the main avenue.

Many IoT products will be covered by specific legislation, but some electronic products with a voltage under 50 volts and ancillary products IoT developers may design and manufacture could fall fully under this directive.

The GPSD complements specific legislation in some areas, applying partially to all products used by consumers, including second-hand. For example, it allows enforcement authorities to deal with all suppliers of a product, not just the main distributor, as in the case of the product directives.[130]

[96] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ('framework directive')

[97] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive)

[98] Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)

[99] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)

[100] 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).

[101] REGULATION (EC) No 1211/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office

[102] REGULATION (EU) No 531/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2012 on roaming on public mobile communications networks within the Union (recast)

[103] European Telecommunications Network Operators' Association. (n.d.). ETNO policy paper towards a telecommunications framework. Retrieved November 28, 2017, from https://etno.eu/datas/publications/studies/2016_Summary_TelcoFrameworkReview.pdf

[104] KPN. (n.d.). Infrastructure-based competition – The case of the Netherlands. Retrieved November 28, 2017, from http://ec.europa.eu/competition/sectors/telecommunications/archive/inquiries/local_loop/kuisch_kpn.pdf

[105] Lucius, von, J. (2016, September 22). EU „Connectivity Package" to reshape telecoms regulation | Noerr LLP. Retrieved November 28, 2017, from https://www.noerr.com/en/newsroom/News/eu-%E2%80%9Econnectivity-package%E2%80%9C-to-reshape-telecoms-regulation.aspx

[106] Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) – COM(2016)590

[107] as above.

[108] GSMA. (2017, June 8). Mobile Industry Calls for Greater Ambition on Telecoms Framework Reforms. Retrieved November 28, 2017, from https://www.gsma.com/gsmaeurope/positions-and-publications/mobile-industry-calls-greater-ambition-telecoms-framework-reforms/

[109] 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)

[110] Härting. (2017, October 19). Study on the Impact of the Proposed ePrivacy Regulation. Retrieved November 28, 2017, from https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/epr_-_gutachten-final-4.0_3_.pdf

[111] BEREC. (n.d.). All you need to know about Net Neutrality rules in the EU. Retrieved November 28, 2017, from http://berec.europa.eu/eng/netneutrality/

[112] REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union

[113] Marsden, C. (2017, October 14). Net neutrality in Europe: Dutch NRA: T-Mobile may continue to violate net neutrality – Bits of Freedom. Retrieved November 28, 2017, from http://chrismarsden.blogspot.com/2017/10/dutch-nra-t-mobile-may-continue-to.html

[114] BEREC. BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules (2016).

[115] Finley, K. (2017, June 6). The End of Net Neutrality Could Shackle the Internet of Things. Retrieved November 28, 2017, from https://www.wired.com/2017/06/end-net-neutrality-shackle-internet-things/

[116] https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en

[117] http://www.emcia.org/documents/K1%202016.pdf

[118] European Commission. (n.d.). Guidance documents to assist stakeholders in implementing directives related to medical devices. Retrieved November 28, 2017, from https://ec.europa.eu/growth/sectors/medical-devices/guidance

[119] COMMISSION NOTICE The 'Blue Guide' on the implementation of EU products rules 2016 (Text with EEA relevance) (2016/C 272/01)

[120] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC

[121] ETSI. (2016). *ETSI EG 203 367 V1.1.1 – Guide to the application of harmonised standards covering articles 3.1b and 3.2 of the Directive 2014/53/EU (RED) to multi-radio and combined radio and non-radio equipment*

[122] European Commission. (n.d.). LIST OF BODIES NOTIFIED UNDER DIRECTIVE : 2014/53/EU Radio equipment. Retrieved November 28, 2017, from http://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction=directive.pdf&refe_cd=2014%2F53%2FEU&requesttimeout=900

[123] European Commission. (2017, May 19). Guide to the Radio Equipment Directive 2014/53/EU. Retrieved November 28, 2017, from http://ec.europa.eu/docsroom/documents/23321

[124] FSFE. (n.d.). EU Radio Lockdown Directive. Retrieved November 28, 2017, from https://fsfe.org/activities/radiodirective/radiodirective.html

[125] Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision)

[126] DIRECTIVE 2014/35/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits (recast)

[127] Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast)

[128] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety

[129] Procedure 2013/0049/COD COM (2013) 78: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on consumer product safety and repealing Council Directive 87/357/EEC and Directive 2001/95/EC

[130] Conformance. (n.d.). General Product Safety directive. Retrieved November 28, 2017, from https://www.conformance.co.uk/adirectives/doku.php?id=generalprod

7. Sector-specific regulatory considerations

In the sections below we consider some sector-specific regulatory considerations that have additional layers of regulatory oversight. These include home automation, children's toys, health and medial devices. These are examples of the more common sectors for IoT innovation but it is important to pay attention to additional regulatory oversight in other heavily regulated areas such as finance or transport as well.

7.1 Home Automation

An important area of standardisation and interoperability is the connection of devices in the home. This involves direct consumer choice, while most of the other standards discussed previously would be mainly invisible to end users.

This is one area where there is little convergence, with several distinct systems. Several are based on the IETF low power personal network standards, while others have their own networking technology at lower layers and may be very difficult to make interoperable.

There are open source implementations for most of these standards with clear efforts being made to attract developers.

7.2 Thread

Thread[131] is a networking protocol developed by Nest, who produce home automation appliances and is part of the Google/Alphabet conglomerate, and backed by several companies including chip developers Arm, Texas Instruments, Silicon Labs and Qualcomm.

The royalty-free protocol is designed for the home and is based on various standards including IEEE802.15.4, IPv6 and 6LoWPAN to provide a low range mesh networking. As in other cases, security figures prominently, with all connections being encrypted.

The group runs a certification programme, which is one of the common activities that successful consortia engage in. Similarly, the group has published their framework as open source.[122]

7.3 Zigbee

The Zigbee standard was developed in 2002 and is one of the most popular. It is based on the same IEEE wireless networking protocols as Thread and also targets the home environment.

The standard sits atop the IEEE 802.15.4 low power standard at OSI layer 2, but it uses its own packet routing protocol at the network layer.[133] This is incompatible with the Internet Protocol, which severely limits its expandability but can provide security as authentication and encryption happen at a fairly low level.

The Zigbee alliance maintains the open standards, made available on Reasonable And Non-Discriminatory (RAND) basis, and provides certification services. It is mainly run by industrial groups, including Chinese giant Huawei, not internet companies and is supported by dozens of manufacturers. Many businesses such as Samsung participate and support several standards and protocols.[134]

The alliance has also developed Zigbee IP,[135] as an open internet compatible protocol based on IETF's 6LoWPAN and other specific technologies.[136]

The consortium is also developing an application layer protocol called Dotdot[137] to simplify interoperability for developers.

7.4 Z-wave

The widespread Z-wave wireless communication standard for home automation is similar to Zigbee in some aspects, and is also supported by an alliance of a large number of companies, including Huawei and many others that also support Zigbee. The Z-wave protocol is, however, quite different from a technical perspective, being based on a different standard for the lower OSI layers.

The system is the proprietary technology of Sigma Designs, which has so far manufactured most of the chips. Some parts have been made available as open source,[138] and the device specifications have been made available, including as the ITU[139] standard. Manufacturers that want to build commercial Z-wave devices must go through the alliance's certification process however.

7.5 Bluetooth

The new Bluetooth Low-Energy (BLE)[140] – or Bluetooth Smart, as it is sometimes known – is a protocol for IoT applications. It offers similar range to Bluetooth but with reduced power consumption. BLE has a major advantage in that the technology is already integrated in smartphones and many other mobile devices and computers. The newer versions of BLE allow sensors to access the Internet directly via 6LoWPAN connectivity. Latest developers include the capacity to form mesh networks with Bluetooth devices, in direct competition with Thread.

The Bluetooth Special Interest Group has thousands of members and provides certification and technical conformity testing services. It is probably the most advanced in this aspect, as Bluetooth devices are widespread. Free membership gives a right to use the IP and trademarks, while paid membership allows participation in technical developments.

Bluetooth technology is very relevant for wearable technology and if successful it could become important for home automation.

7.6 Toy Safety

In Europe, toys fall within the scope of multiple standards and directives. Electronic and radio enabled toys will have to comply with technical regulations described in the previous section.[142] Specific toy safety is covered under a Toy Safety Directive 2009/48/EC, which is also part of the New Legislative framework. The directive covers basic safety with an additional focus on the use of chemicals such as heavy metals (mercury, lead), allergens and substances likely to cause cancer, genetic or reproductive harms.

Specific standards for electronic toy safety are set out by CENELEC under EN 62115,[143] which covers toy computers. Many IoT products marketed to children could be covered by toy regulations. The Norwegian Consumer Council has carried out extensive work on connected toys, mainly focusing on the privacy aspects.[144]

7.7 Sector Specific Regulation

Some IoT sectors are covered by specific regulations that require extensive specialist advice. Cars and medical devices are two such examples.

Motor vehicles

According to reports, it is expected that by 2020 some 90% of new cars will be connected to "the internet".[145] It is possible that the actual number will be lower, and that the internet will be reduced to a corporate closed network. In any case, cars are poised to be a major area for IoT. Motor vehicles have been subjected to extensive controls over safety, competition and emissions for decades.[146] The regulations are incredibly complex. Particularly relevant for IoT developers is the Motor vehicles (Regulation (EC) 661/2009),[147] which provides an update to the safety requirements to some of the newer technologies such as lane departure warning, and repeals many old pieces of legislation.

The new challenges of self-driving cars will require an update to some of these rules.[148] There is currently no EU law on autonomous vehicles, but certain countries are already taking the initiative. The UK, for example, is considering a Vehicle Technology and Aviation Bill that will regulate liability and responsibility,[149] ensuring that nobody is left without insurance cover in the event of an accident.

7.8 Health and Medical Devices

Health and medical devices are highly regulated, and IoT developers can easily encounter legal obstacles. Google's Deepmind artificial intelligence company developed a tool for doctors to improve their workflow and decision making, but was forced to stop using[150] the tool after failing to register it as a medical device with the UK Medicines & Healthcare products Regulatory Agency.

Even a cursory overview of this regulatory landscape -which involves various directives, and European standards – is beyond the scope of this overview of IoT policy, standards, and regulation. The overall approach is similar to other New legislative framework safety areas around conformity and standards. Several useful summaries can be found online.[151]

7.9 European Standards Organisations

As discussed above, ESOs have a central role in setting detailed technical specifications. In the field of radio, the process involves a triangular relation of the Commission, the European Conference of Postal and Telecommunications Administrations (CEPT), particularly its Electronic Communications Committee (ECC), and ETSI.

National authorities manage radio spectrum at the country level within the EU, and adopt a national table of radio spectrum allocations, and assign radio spectrum to the various users via individual or general authorisations. These could include mobile spectrum auctions or giving free access to unused frequencies.

Developers wishing to operate at a particular radio frequency without obtaining tried and tested equipment may need to check whether there is specific relevant decision through the public ECC database and search for the relevant harmonised standards at the ETSI website. The CEPT has produced – via the European Radio Office – Recommendation 70-03 r*elating to the use of short range devices* which describes in tables the regulations and conditions for use of various categories of radios relevant to IoT.[153]

[131] Thread Group. (n.d.). Home. Retrieved November 27, 2017, from https://threadgroup.org/

[132] Openthread. (n.d.). Openthread. Retrieved November 28, 2017, from https://github.com/openthread/openthread

[133] Gascón, D. (2009, April 28). 802.15.4 vs ZigBee | Libelium. Retrieved November 28, 2017, from http://www.libelium.com/802-15-4-vs-zigbee/

[134] Sharp, K. (2017, February 16). IoT 201: ZigBee and Thread mesh networks – ARTIK IoT Platform. Retrieved November 28, 2017, from https://www.artik.io/blog/2017/02/iot-201-zigbee-and-thread-mesh-networks/

[135] Zigbee Alliance. (n.d.). Zigbee IP and 920IP. Retrieved November 27, 2017, from http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeeip/

[136] Cragie, R. (n.d.). ZigBee IP update – IETF 87 Berlin. Retrieved November 28, 2017, from https://www.ietf.org/proceedings/87/slides/slides-87-lwig-6.pdf

[137] Zigbee Alliance. (n.d.). the dotdot story. Retrieved November 28, 2017, from https://www.speakdotdot.com/dotdotstory/

[138] OpenZWave. (n.d.). OZW Utilities. Retrieved November 28, 2017, from http://www.openzwave.com/

[139] ITU. (2015). *G.9959 : Short range narrow-band digital radiocommunication transceivers – PHY, MAC, SAR and LLC layer specifications*. itu.int.

[140] Bluetooth SIG. (n.d.). Bluetooth Technology Website. Retrieved November 28, 2017, from https://www.bluetooth.com/

[141] BTHA. (n.d.). Directives and legislation related to Toys. Retrieved November 28, 2017, from http://www.btha.co.uk/wp-content/uploads/2017/04/Directives-and-legislation-related-to-Toys-WEBSITE-version.pdf

[142] SGS. (n.d.). Electrical and Electronic Toys. Retrieved November 28, 2017, from http://www.sgs.com/-/media/global/documents/brochures/sgs-crs-electrical-and-electronic-toy-services-a4-en-16-v1.pdf

[143] Engineering360. (n.d.). CENELEC – EN 62115 – Electric toys – Safety. Retrieved November 28, 2017, from http://standards.globalspec.com/std/9898531/cenelec-en-62115

[144] Johnsen, A. (2016). *Investigation of privacy and security issues with smart toys.* forbrukerradet.no.

[145] Telefonica. (2013, June 24). 90% of new cars will be connected by 2020. Retrieved November 28, 2017, from https://iot.telefonica.com/blog/90-of-new-cars-will-be-connected-by-2020

[146] European Commission. (n.d.). Directives and regulations on motor vehicles, their trailers, systems and components. Retrieved November 28, 2017, from https://ec.europa.eu/growth/sectors/automotive/legislation/motor-vehicles-trailers_en

[147] REGULATION (EC) No 661/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 July 2009 concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefore

[148] Pinsent Masons. (2017). Connected autonomous vehicles: the emerging legal challenge. Retrieved November 28, 2017, from https://www.pinsentmasons.com/PDF/2017/Freedom-to-Succeed-AMT/Connected-autonomous-vehicles-report-2017.pdf

[149] Vehicle Technology and Aviation Bill (HC Bill 143)

[150] Lomas, N. (2016, July 20). DeepMind's first NHS health app faces more regulatory bumps. Retrieved November 28, 2017, from http://social.techcrunch.com/2016/07/20/deepminds-first-nhs-health-app-faces-more-regulatory-bumps/

[151] Crossley, S. (n.d.). EU regulation of health information technology, software and mobile apps | Practical Law. Retrieved November 28, 2017, from https://uk.practicallaw.thomsonreuters.com/2-619-5533?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

[152] European Communications Office. (n.d.). ECO Documentation v5.1. Retrieved November 28, 2017, from http://www.ecodocdb.dk/

[153] CEPT. (2017). *ERC Recommendation 70-03 Relating to the use of Short Range Devices (SRD).* erodocdb.dk.

8. Telecoms Issues in IoT

The regulatory framework described above has already raised specific issues for IoT developments. The regulatory umbrella body for European telecoms BEREC reported in 2016 the main potential obstacles for IoT as: spectrum, identifiers – which include IP addresses, security, roaming and the Electronic Communications Code categories we discussed previously.[154] Most of these issues relate to IoT connected through mobile telephony networks.

General connectivity and the broader development of mobile technologies such as 5G have also been addressed in various papers.[155]

Connectivity

As discussed in the standards section, one of the key issues in IoT will be the development of technologies that can connect devices directly via long range networking potentially bypassing the current telecoms networks of fibre optic and copper. The combination of long distance networking with more flexible low power home and portable networks could promote more decentralised technologies and increase privacy. In view of these developments mobile companies have rushed to upgrade their existing cellular infrastructure to provide similar functionalities.

The most important policy issue in this area will be the development of 5G mobile networks, which, starting in 2010, promises to bring unprecedented speed, low latency, and hyper-connectivity that will squeeze many more connections into the available bandwidth.[156] This is specifically designed to benefit not just consumers and media but industrial areas such as self-driving cars or remote medicine.

5G will provide many technical advantages to support independent developers, but there could be challenges if bandwidth is not allocated fairly. 5G will have reserved capacity for industry verticals on transport, energy, etc. During the discussions on net neutrality telecoms companies threatened to pull out investments in 5G if rules forced them to give equal access to their networks to all parties, despite current rules excluding M2M data traffic. This could prove problematic for independent developers, for example, a community bike sharing scheme trying to access the transport vertical dominated by competitors such as car manufacturers and transit authorities.

8.1 Subscriptions and Switching

Another issue, perhaps more relevant to larger developers, is the management of subscriptions for large sensor networks. Companies operating smart meters or smart city systems could require thousands of devices, and in many cases mobile companies are not prepared to deal with their needs to be able to monitor connections and manage subscriptions flexibly.

Switching operators is another issue. At present vendor lock-in is a concern because changing providers normally requires either swapping a SIM card or other hardware. The cost of dispatching technicians to deal with this can make it unprofitable, leading to lock-in or potentially an environmentally costly disposal of units, which companies will simply replace if their cost is low.

Technical solutions to this problem could involve enabling remote management of the SIMs. The GSMA has defined a specification for the remote management of embedded SIMs specifically for M2M communications.[157]

Organisational solutions would involve allowing IoT networks to become their own virtual mobile networks, buying bulk access from infrastructure providers but having their own Mobile Network Code,[158] similarly to how supermarkets mobile offers operate. It is unclear how this would operate without lock-in at the infrastructure level, and there is already scarcity of network codes, which are limited to three digits.

Both solutions are not mature and BEREC believes that smaller IoT operators may not have market power to drive these changes. Changes to An evolution of Art. 30 of the Universal Service Directive entitled “Facilitating change of provider” might be appropriate to grant IoT users the right to switch remotely.[159]

8.2 Roaming

The applicability of EU roaming regulations to IoT devices operating on mobile networks can have important implications, particularly for transport but also for many portable devices. At present low power networks are not subjected to roaming, but this could change in the future.

The international use of the ITU standard E.164 telephone numbering system provides the basic interoperability of roaming, and enables the use of SIM cards to operate across borders.

According to BEREC,[160] the basic roaming obligations around temporary travelling to another country clearly apply to IoT devices. A different situation applies to permanent roaming. This could include devices that are sold outside the country of production but use a SIM from the country of production (e.g. cars, e-readers), or where a foreign network provides better coverage of border areas.

There is no clear guidance on permanent roaming,[161] which in principle would not be covered by regulations. If that is the case, operators can set out specific conditions and could even prohibit permanent roaming altogether. BEREC guidance on roaming simply says that each case needs to be considered on its own terms. Regulators and industry have asked for more clarification on this issue.[162]

8.3 Numbering and Addressing

The large numbers of IoT devices creates a problem as these need to be identified uniquely, ideally at the global level. The internet at large already suffers from a shortage of internet addresses, which the newer IPv6 will eventually solve. Unfortunately, the implementation of IPv6 has been delayed by issues of backwards compatibility and a lack of policy direction. Another proposed identifier for at least some IoT systems based on mobile telephony is the IMSI number, under recommendation by ITU-T E.212 *for the international identification plan for public networks and subscriptions*.[183]

While the potential shortage for addresses is there, in practice, the telecoms industry body ETNO considers that there is no need for the time being to strengthen regulations at the European level and these issues are better dealt at the national level.

8.4 Spectrum

Scarcity of spectrum is an ongoing long-term problem given the continued growth of communications systems, and IoT is one of the areas where there is growing demand. IoT devices can use many types of radio frequencies, from short range to very long range, mobile, or even FM radio ranges.

The use of free unlicensed spectrum is the most important element for innovation independent from established telecoms industries. This is typically through the Industrial, Scientific and Medical (ISM) bands. As noted previously, the development of low power long range networking, for example, has been enabled by free unlicensed access, and the widespread adoption of wifi is premised on similar circumstances.

Unlicensed spectrum for short range is harmonised through the CEPT/ERC Recommendation 70-03 (SRD). There are also experiments to give access to unused spectrum near TV bands. Other discussions around spectrum in IoT are tied to developments in mobile telephony.

The Radio Spectrum Policy Group from the European Commission has studied the requirements of spectrum for IoT and concluded that allocating specific bands for IoT is not necessary but further access should be enabled by various means, including increasing unlicensed access.

The groups however point out that “making IoT stakeholders aware of their options for accessing spectrum is a challenge, as these may not be familiar with spectrum management regimes, availability of frequencies and conditions of use.” [164]

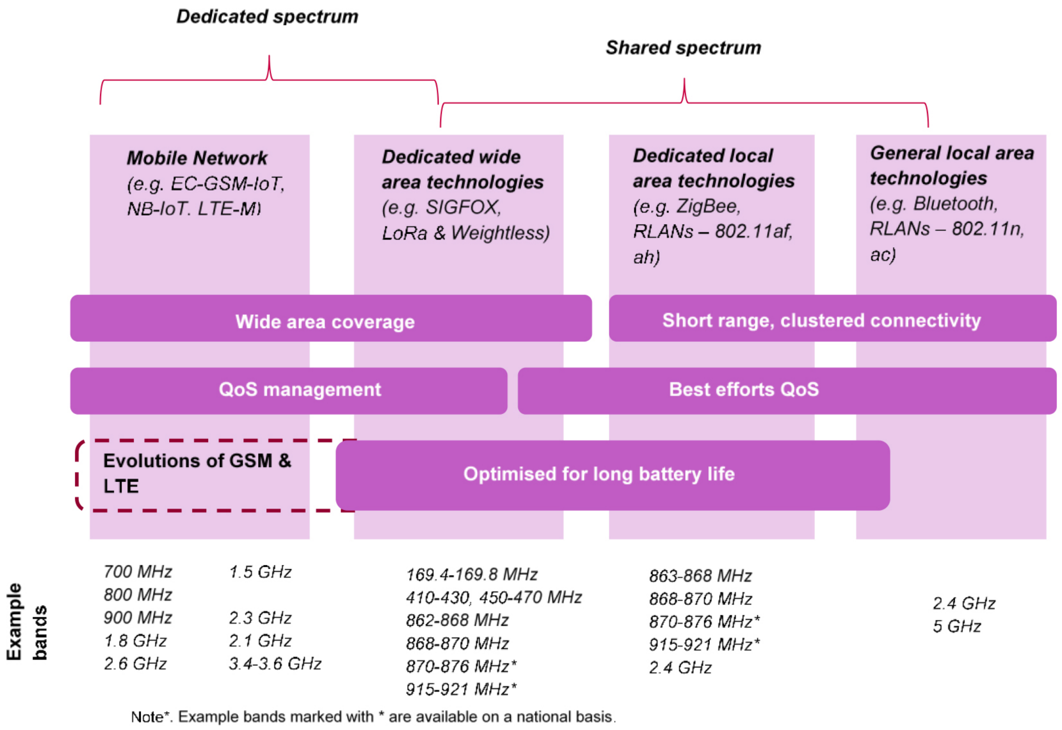
Dedicated spectrum
Shared spectrum
Mobile Network (e.g. EC-GSM-IoT, NB-IoT. LTE-M)
Dedicated wide area technologies (e.g. SIGFOX, LoRa & Weightless)
Dedicated local area technologies (e.g. ZigBee, RLANs – 802.11af, ah)
General local area technologies (e.g. Bluetooth, RLANs – 802.11n, ac)
Wide area coverage
Short range, clustered connectivity
QoS management
Best efforts QoS
Evolutions of GSM & LTE
Optimised for long battery life
Example bands
700 MHz
800 MHz
900 MHz
1.8 GHz
2.6 GHz
1.5 GHz
2.3 GHz
2.1 GHz
3.4-3.6 GHz
169.4-169.8 MHz
410-430, 450-470 MHz
862-868 MHz
868-870 MHz
870-876 MHz*
915-921 MHz*
863-868 MHz
868-870 MHz
870-876 MHz*
915-921 MHz*
2.4 GHz
2.4 GHz
5 GHz
Note*. Example bands marked with * are available on a national basis.

Figure 6[165]

[154] BEREC. (2016). *BEREC Report on Enabling the Internet of Things.* berec.europa.eu.

[155] Brown, I. (2015). *GSR discussion paper: Regulation and the Internet of Things.* itu.int.

[156] Hellemans, A. (2015, May 20). Why IoT Needs 5G. Retrieved November 28, 2017, from https://spectrum.ieee.org/tech-talk/computing/networks/5g-taking-stock

[157] GSMA. (2013). *Embedded SIM Remote Provisioning Architecture Version 1.1*

[158] TELETOPIX.ORG. (2012, December 17). What is MNC and MCC for GSM. Retrieved November 28, 2017, from http://www.teletopix.org/gsm/what-is-mnc-and-mcc-for-gsm/

[159] BEREC. (2016). *BEREC Report on Enabling the Internet of Things.* berec.europa.eu. (p. 32)

[160] ibid.

[161] EY. (2015). *Enabling the IoT environment. EY Inside Telecommunications*, (17).

[162] Guthfreund-Roland, F., & Hallé, M. (2017, September 13). Are EU regulations on Union-wide roaming services applicable to IoT connectivity services? Retrieved November 28, 2017, from https://www.dlapiper.com/en/france/insights/publications/2017/09/eu-regulations-on-roaming-services/

[163] ITU. (2016). *E.212 : The international identification plan for public networks and subscriptions.* itu.int.

[164] RADIO SPECTRUM POLICY GROUP. *RSPG17-006 FINAL Opinion on the Spectrum Aspects of the Internet-of-things (IoT) including M2M*, circabc.europa.eu.

[165] ibid.

9. Practical Issues for Electrical IoT Devices

Below we give some examples of the kinds of practical issues around electrical regulation that IoT developers may need to consider. This is not an exhaustive list.

9.1 Smart Grids

IoT devices need to comply with electromagnetic regulations, but many IoT products are not just passive consumers of electricity and are actively involved in managing their consumption or the home, or even the wider electrical grid. Smart meters are the most obvious element but smart appliances of all kinds with energy management are in the pipeline.

There are many projects to develop smart grids, based on smart devices and decentralised power production through solar or other renewables.[166] Cybersecurity is seen as one of the main challenges, despite assurances from the electrical industry.[167] However, basic electrical compliance and good engineering cannot be taken for granted to assure the safety of users and interacting equipment; and the general stability of electricity supply under variable loads.

9.2 Power Supplies

The humble and ubiquitous power supply unit is one of the most important components in an IoT device from the point of view of safety. Tests of power supplies regularly show a huge variability in quality with a concerning number of systems being dangerous to consumers.[168]

Common issues include under or over voltage, transient spikes and complex distortions of electrical signals that can damage components and also cause humming noise[169] affecting AV equipment. Cheap or missing safety-critical components, bad wiring and cheap material can make it very easy for power supplies to not only electrocute their users but also cause fires.[170] Energy efficiency is another important aspect,[171] with the US currently having the highest requirements.

Responsible sourcing of components is an ethical issue for any IoT developer, but probably not more so than in power supplies.

Plugs and socket outlets are not covered by the LVD, but there are various standards that must be followed.

9.3 Labelling

Product identification and traceability require the labelling of components and finished products. Even Apple is forced to break its minimalist design to include product information and logos, although it has lobbied extensively to change this in countries such as India.[172]

Some IOT devices may require even further information and weather resistant rip-proof labels.[173] Someone finding a low power device a decade after it was installed may need some information about what the thing is doing without the need to open it and perform some forensics.

The US has reduced the labelling requirements for electronics, with the E-Label Act[174] that allows for information to be displayed electronically.[175] The EU maintains strong labelling requirements, the most important of which is the CE marking.

9.4 CE Marking

The letters CE (in a logo with a rounded E) are affixed to most products – including electronic IoT devices – sold in the EU, signifying the manufacturer's declaration that the product fully complies with the essential requirements of the relevant product directives. The mark in principle indicates to relevant authorities that the product can be legally placed in the European single market. The letters are the abbreviation of French phrase *Conformité Européene*.[176]

The process to follow in order to be able to label a product with the CE mark is explained in the Blue Guide, as it is part of the general compliance procedures, that include identifying relevant legislation, testing for conformity and drawing the appropriate documentation.

The label is the responsibility of the manufacturer, but distributors should ensure that the supporting documentations matches the conformity. CE marking should only be attached to products that fall under the scope of one of the product directives that mandate its affixing.[177]

9.5 Consumer Protection

Consumer organisations, such as Consumers International, have raised concerns about the Internet of Things.[178] These include difficulties determining liability in complex webs of products and companies, privacy and security, and exacerbating current network effects and monopolies in the tech sector. Other concerns are specific to hybrid products that include hardware and software, which can be remotely controlled, and where it is unclear whether the notion of ownership applies anymore.[179] These issues if unchecked will lead to vendor lock-in through lack of interoperability and a lack of choice.

Other discussions[180] have covered the difficulty of defining the scope of consumer issues with IoT, particularly around the use of data in smart cities or for public benefit projects, such as use of location data for smart city management, where issues could rather be framed under citizenship and democracy.

General consumer protections still apply, though, as these are enshrined at the highest levels of EU law, including article 38 of the Charter of Fundamental Rights.[181] These are based on the principles of fair treatment, products meeting basic standards and a right of redress. The Directive on Consumer Rights (2011/83/EU)[182] gives consumer specific powers, such as being able to return goods, improved transparency, including about compatibility of hardware and software that can be particularly relevant to IoT.

The EU considers consumer protection a critical aspect, as it was first conceived as a single market, rather than a polity. There are various other pieces of legislation and initiatives summarised in the European Consumer Agenda.[183] However, it would be fair to say that in relation to privacy, competition law or technical regulations, consumer law is underdeveloped and lacks the enforcement tools available in other areas.

9.6 Liability

The legal basis of product liability law in Europe is Product Liability Directive 85/374/EC[184] (PLD), which establishes the principle that the producer of a product is liable for damages caused by a defect in his producer. This is a principle of no-fault liability where the producer will be liable even if he proves he was not negligent or a third person contributed to the damage caused.

The concept of producer is broader than the manufacturer under the New Legislative Framework Directives, meaning that action can be taken against any actor in the supply chain responsible for a fault, in many case this could be the importer.

The fundamental problem here is that the PLD excludes services, and all IoT products contain a software element that is provided under license as a service. The extension of the Product Liability Directive to services would seem the logical step, but this is fiercely resisted by most of the IT industry. Our ethnographic research shows that IoT developers are also part of this trend and oppose any extension of liability. In addition, this could cause unforeseeable damages to open source projects freely distributed and to independent developers.

In addition to the software problem, IoT exacerbates existing problems to allocate responsibility and to prove causal links for defects or negligence as systems grow in complexity. A small point is that liability stops after 10 years, while some IoT devices are designed with a battery life expectancy of over 10 years.

The European Commission carried out a public consultation on the functioning of the PLD in 2017, with explicit reference to IoT issues. The responses showed the need to take action but the Commission has not indicated yet what changes they may propose.[185] Liability for self-driving cars is already being worked out at the national level in various countries.

9.7 Environmental regulation of electronics

Environmental regulations for electronics or white goods will equally apply to IoT devices. The main applicable legislations are:

Regulation (EC) No 1907/2006 of the European Parliament and of the Council on the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH)[186]

The REACH Regulation sets out a classification of chemicals, controls, and registration procedures. It is unlikely IoT developers will deal with these directly, but in some cases controlled chemicals could be incorporated in components – e.g. scented toys, lead ballast or plastics – and developers should comply.

Restriction of Hazardous Substances in Electronic Equipment Directive 2011/65/EU (RoHS 2)[187]

The RoHS aims to ensure that certain chemicals – six metals and fire retardants – are completely excluded from electronic equipment, and it certainly covers all IoT devices.

The RoHS requirements apply to end products but manufacturers must ensure that components do not contain any of the restricted substances above the defined maximum concentration values. A technical report must be produced by the component manufacturer containing the analysis and component data and be kept on file by the producer of the finished product. For IoT developers in practice this means working with certified suppliers.

Waste Electrical & Electronic Equipment Directive 2012/19/EU (WEEE)[188]

The Directive on waste electrical and electronic equipment makes producers of electronic and electrical goods responsible for financing their recovery and recycling. Producers pay a fee to support infrastructure that allows users to recycle waste products. The Directive could also have an impact on the design of products to make recycling easier by separating materials.[189]

Environmental regulations on electronics seem to have delivered some positive results,[190] but its effect on IoT are yet to be seen. Infrastructure electronics in smart cities and buildings could prove a considerable challenge.

The environmental group Greenpeace maintains a ranking of green electronics that compares large firms along several criteria: use of energy, resource consumption and chemicals. The guide shows that there is still way to go.[191] Greenpeace looks at the sustainability of the design, including the ease of repairs and part replacement.

9.8 Labour

A 2012 report found that the electronics sector had the worst labour conditions of any industry.[192] Fast turnover rates and the sheer speed of the sector force workers into long hours and unhealthy practices. In addition, it has long been known that the supply chain of the materials required in modern electronics has led to untold damage in Central Africa and other areas. The situation has not improved substantially, and in 2016 NGOs requested that cobalt was added to the list of conflict minerals.[193]

The Clean Electronics Production Network (CEPN) was launched in 2016 to reduce exposure to hazardous materials by workers in the electronics supply chain.[194] The development of ethical supply chains is advancing slowly, led among others by Dutch NGO and phone manufacturer Fairphone.[195]

There are not as yet specific regulation on labour conditions, and developers will have to look at initiatives such as the above for guidance.

[166] Grant, C., McCue, J., & Young, R. (2015). *The power is on: How IoT technology is driving energy innovation. Deloitte University Press.*

[167] Corfield, G. (2016, October 25). Existing security standards are fine for IoT gizmos in electrical grids. Retrieved November 28, 2017, from https://www.theregister.co.uk/2016/10/25/iot_in_electrical_grids_what_could_possibly_go_wrong/

[168] Engdahl, T. (2016, January 25). Power supply teardowns reveal safety issues. Retrieved November 28, 2017, from http://www.epanorama.net/newepa/2016/01/25/power-supply-teardowns-reveal-safety-issues/

[169] Captech. (n.d.). Common issues with power supply. Retrieved November 28, 2017, from https://www.captech.com.au/2016/05/06/common-issues-with-power-supply/

[170] Mammano, B., & Bahra, L. (2005). *SEM1600 Topic 1: Safety Considerations in Power Supply Design. Texas Instruments.*

[171] CUI Inc. (2016). *Efficiency Standards for External Power Supplies.* cui.com.

[172] Chitravanshi, R. (2016, December 29). Apple seeks relaxed labelling rules, doesn't want to print product info on devices. Retrieved November 28, 2017, from https://economictimes.indiatimes.com/tech/hardware/apple-seeks-relaxed-labelling-rules-doesnt-want-to-print-product-info-on-devices/articleshow/56229190.cms

[173] Labels and their importance in the electrical industry. (2017) *Electrical Trade Magazine.*

[174] US government act S. 2583 (113th): E-LABEL Act

[175] Eggerton, J. (2017, July 13). FCC Votes to Implement E-LABEL Act | Broadcasting & Cable. Retrieved November 28, 2017, from http://www.broadcastingcable.com/news/washington/fcc-votes-implement-e-label-act/167120

[176] CE-marking.org. (n.d.). What is CE Marking (CE mark)? Retrieved November 28, 2017, from http://www.ce-marking.org/what-is-ce-marking.html

[177] European Commission. (n.d.). Manufacturers – Growth – European Commission. Retrieved November 28, 2017, from https://ec.europa.eu/growth/single-market/ce-marking/manufacturers_en

[178] Consumers International. (2016). *The Internet of Things and challenges for consumer protection.*

[179] Perzanowski, A. & Schultz, J., (2016). The End of Ownership. MIT Press.

[180] Milne, C. (2016, June 1). Internet of Things, consumers and the public interest. Retrieved November 28, 2017, from http://blogs.lse.ac.uk/mediapolicyproject/2016/06/01/internet-of-things-consumers-and-the-public-interest/

[181] Charter of Fundamental Rights of The European Union (2010/C 83/02)

[182] Directive 2011/83/EU of The European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council

[183] COM(2012) 225 Final Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A European Consumer Agenda – Boosting confidence and growth

[184] 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

[185] European Commission. (n.d.). Public consultation on the rules on liability of the producer for damage caused by a defective product – Growth – European Commission. Retrieved November 28, 2017, from http://ec.europa.eu/growth/content/public-consultation-rules-liability-producer-damage-caused-defective-product-0_en

[186] REGULATION (EC) No 1907/2006 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC

[187] DIRECTIVE 2011/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

[188] DIRECTIVE 2012/19/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 July 2012 on waste electrical and electronic equipment (WEEE)

[189] Conformance. (n.d.). Waste Electrical and Electronic Equipment (WEEE) directive. Retrieved November 28, 2017, from https://www.conformance.co.uk/adirectives/doku.php?id=weee

[190] Ciocci , R, Pecht, M. (2006) "Impact of environmental regulations on green electronics manufacture", Microelectronics International, Vol. 23 Issue: 2, pp.45-50,

10. Intellectual Property

Intellectual property will be an important issue for all IoT developers, from avoiding infringing other people's rights, to managing theirs in their own creations. The use of frameworks and standards can also complicate the picture, as many of these will have some licences with restrictions. These may allow, for example, the development of test kits but require extra steps and licensing to go into manufacture or use the project logo and brand.

IP also has implications from an ethical point of view. The use of open source technologies is widespread in consumer IoT, which could allow for the easier transfer of technologies to disadvantaged groups or countries.

Issues around ownership of devices, raised by consumer groups, have their root in intellectual property arrangements, with particular problems raised by Digital Rights Management (DRM) technologies. These concerns were also raised at an expert workshop on citizen/consumer engagement with policy-making for the Internet of Things attended by VIRT-EU researchers, which took place in London on June 13, 2017.

Software directive

Copyright protects the creativity and originality of authors, and software as written code is protected by copyright, but its concepts, functionalities or algorithms are not. The copyright of computer programmes in the EU is treated differently from that of other creative works. Directive 2009/24/EC on the Legal Protection of Computer Programs[196] provides the main basis. The directive contains provisions for the reverse engineering of software to ensure compatibility under certain limited conditions, which could be important in IoT.

10.1 Infosoc Directive

IoT designs for hardware could be protected by copyright as well. In this case, the mainstream copyright provisions will apply. Here the main piece of legislation is Directive 2001/29/EC *on the harmonisation of certain aspects of copyright and related rights in the information society*.[197]

Copyright legislation puts extra protections against the removal of technical protection measures for digital rights management (DRM). DRM has, for example, stopped US farmers from repairing or modifying their own tractors, among many other cases. These issues were raised at the expert workshop on consumer engagement mentioned above.

10.2 Patents

Patents protect inventions for a limited time in order to promote their disclosure to the wider public. Inventions have to be novel and useful and cannot be simply ideas but must include some form of practical embodiment to show they are feasible. Patents are the bread and butter of industry and innovation, but in high tech electronics have become a brake on developments.

Companies use patents not just to protect their innovations but to stop others from innovating. In some cases, patents are used as currency in cross licensing deals. Portfolios of thousands of patents are traded in complex schemes, and a single new piece of technology could involve hundreds of patents from myriad companies, including competitors.

Patents in Europe cannot cover software, meaning its functionality and algorithms as code is covered by copyright, unless this is embedded as integral parts of a hardware development.

Hardware and software integration is prime IoT territory, and the framework around this can be problematic for independent developers. In many cases, developers will be either working on software, and accessing basic hardware technologies, either through some open access scheme or standard or a license, and might face problems if they try to innovate in hardware design.

Patent legislation in Europe is extremely complex, with a lot of responsibilities at the national level. Recently, a unitary patent system has been put in place to try to simplify protections across most of Europe.[198]

10.3 Database Directive[199]

Data ownership, access and control are central issues in IoT. Databases can be protected under the EU sui-generis database right.[200] This is a European right to protect the investments in the creation of databases, and as such it is primarily and economic right that belongs to those who put the investment forward. In some cases, contributions from people can be considered investment in kind and they will have a share in the right. This is, for example, how the Openstreetmap collaborative cartography project operates. The right is shorter than copyright and has some exemptions to access small sections of databases. Issues of data ownership and rights have arisen in every field site VIRT-EU researchers have visited.

10.4 Open Source

Open source figures prominently in the world of IoT. According to W3C, *91% of IoT developers uses open source software, open hardware, or open data in at least one part of their development stack*.[201] Our field research confirms these figures and the centrality of open source for developers. Open source can reduce costs, attract developers, and allow technologies to expand rapidly. Open source can also provide interoperability as an alternative to standards.

Most systems have some form of open source implementation, with a fairly transparent strategy to attract developers and expand their user base. However, in many cases manufacturers still need to get their products certified and pay consortium fees.

In some cases, the underlying hardware is proprietary. The broader electronics world has seen efforts in recent years to create “open hardware”,[202] which is challenging as the IP rules for physical objects are different from software. Open hardware devices such as the micro controller Arduino are popular in IoT.

10.5 Patents and Standards

Not all IoT systems that claim to be open are fully open despite having an open source implementation. Normally the issue is patents that are licensed under the so-called FRAND terms: fair, reasonable and non-discriminatory.

While this sounds positive, the challenge is that there is no definition of what this means, and could include paying cheap royalties that quickly accumulate in growing projects or force a tax to downstream users. Mobile telephony is plagued by such arrangements, which add substantial costs to handsets, even with open source software such as Android.

FRAND arrangements do not normally allow relicensing to any potential reuse of derived products, being particularly detrimental to true open source projects. The definition of a truly open standard is one which adheres to royalty free and non-discriminatory principles. Royalty-free, non-discriminatory terms lead to standards that are unencumbered by restrictions that can undermine the benefits of openness.[203]

Even if royalties are not demanded, patent holding companies may attach conditions that still have the effect of disadvantaging rivals. It could chill development and restrict the market, for example, where it creates uncertainty. FRAND gives patent owners too much power to determine the evolution and use of the standard. It can be a way for existing market dominant players to retain leverage in the provision of services.

10.6 Property and Rights

Copyright legislation puts extra protections against the removal of technical protection measures for digital rights management (DRM). DRM has, for example, stopped US farmers from repairing or modifying their own tractors,[204] among many other cases. This is based on the idea that although the tractor may belong to the farmer, the software that makes it run is actually licensed form the manufacturer. As a copyright work, it is up to the manufacturer to allow any modifications, and furthermore, as they manufacturer normally employs some DRM technology to stop farmers form tampering with their software, the breaking of such protections is a crime in itself. As mentioned previously, these issues have emerged in our preliminary field work findings.

The regulation of DRM is slightly different in the US and the EU. In Europe, there are some limited cases where reverse engineering software is allowed in order to provide for the interoperability of technical systems, while the US provides some specific exceptions where it is lawful to break DRM, such as “ripping” DVDs.[205] However, neither regime would allow owners to casually modify their products to obtain new or improved functionalities, or to correct faults. This is a problematic issue for consumers in the IoT as well as for developers trying to achieve interoperability, as many manufacturers use DRM to keep competitors at bay.

It is important to understand that DRM is not the same as patent protections, which can achieve similar results for competing businesses, but are less restrictive for users.

10.7 Data Ownership

Data cannot be owned as property in most of the EU. Companies can have rights over data, particularly the database right, but also potentially copyright in the content of the data or even the arrangement and structure of a database. This system sits across any personal rights that individuals may have in that data.

Personal information is covered by data protection, and companies building a database of personal information – say a marketing directory – will have to comply with the law, but these systems operate independently. Whether an individual has a right to be removed from a database trumping the interest of the database owner will have to be examined on a case by case basis.

Non-personal information from sensors, or other devices where individuals cannot be identified, is not covered by data protection, but there are growing concerns that the current framework may not be enough. Individuals have sense of ownership over all the data that their devices generate, and there concerns that individuals can eventually be identified from such unique data linked to their behaviour even in the absence of personal details.

Extending the intellectual property model to give individuals more control could be problematic as this could undermine fundamental rights if the right to data was to be traded. However, increasing the control that individuals have over the data they generate would be positive from the point of view of consumer rights. Discussions about giving individuals more control have been encountered by our researchers at various field sites, such as the London consumer rights expert workshop, events for the the IoT Trustmark, and IoT Week in Geneva.

The European Commission has consulted about creating some form of new right to data for individuals who generate non-personal data in the course of their electronic activities. The commission appears to have abandoned this idea but has proposed a new directive that would promote the free flow of non-personal data by removing localisation requirements and cross-border obstacles.[206]

[191] Greenpeace USA. (2017). *Guide to Greener Electronics* 2017.

[192] Mims, C. (2012, January 9). Electronics Makers Have Worst Labor Practices of Any Industry, Says Report. Retrieved November 28, 2017, from https://www.technologyreview.com/s/426565/electronics-makers-have-worst-labor-practices-of-any-industry-says-report/

[193] LexisNexis Legal & Professional. (2017). *Ethical Sourcing Risks in the Global Electronics Supply Chains | Sustainable Development Goals.* sdgresources.relx.com.

[194] CEPN. (n.d.). Clean Electronics Production Network. Retrieved November 28, 2017, from http://www.centerforsustainabilitysolutions.org/clean-electronics/

[195] Fairphone. (n.d.). Understanding the materials in mobile phones. Retrieved November 28, 2017, from https://www.fairphone.com/en/project/understanding-materials-mobile-phones/

[196] DIRECTIVE 2009/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 April 2009 on the legal protection of computer programs

[197] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

[198] European Commission. (n.d.). Unitary patent. Retrieved November 28, 2017, from https://ec.europa.eu/growth/industry/intellectual-property/patents/unitary-patent_en

[199] DIRECTIVE 96/9/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 1996 on the legal protection of databases

[200] Out-Law (n.d.). Database rights: the basics. Retrieved November 28, 2017, from https://www.out-law.com/page-5698

[201] VisionMobile. (n.d.). *The Essential Guide to Open Source in IoT*. w3.org.

[202] OSHWA. (2012, April 8). About the Open Source Hardware Association. Retrieved November 28, 2017, from https://www.oshwa.org/about/

[203] Open Rights Group. (n.d.). Response to Government Open Standards consultation. Retrieved November 28, 2017, from https://www.openrightsgroup.org/ourwork/reports/open-standards-consultation

[204] Doctorow, C. (2017, April 10). More on the desperate farmers jailbreaking their tractors' DRM to bring in the harvest. Retrieved November 28, 2017, from https://boingboing.net/2017/04/10/tenant-farmers.html

[205] Mcsherry, C., Walsh, K., & Stoltz, M. (2015, October 27). Victory for Users: Librarian of Congress Renews and Expands Protections for Fair Uses. Retrieved November 28, 2017, from https://www.eff.org/deeplinks/2015/10/victory-users-librarian-congress-renews-and-expands-protections-fair-uses

[206] European Commission. (2017). Free flow of non-personal data. Retrieved November 28, 2017, from https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data

11. Security

Security issues in IoT overlap to a large extent with privacy considerations. In addition to the potential risks for personal data there are various security issues specific to IoT.

The risks to infrastructure, such as electrical grids, is a major cybersecurity concern, and IoT devices are one of the potential weak spots. This ability to cause systemic damage beyond an individual device or network has driven governments to put a lot of attention to the security of IoT. To this day computer security regulations are not as developed as those for product safety.

The technologies involved in IoT in themselves have specific security risks. Many IoT devices are small and low powered without a user interface and may be unable to implement common security practices. Smart objects such as fridges can struggle with security information in user interaction. Some of these devices are designed to operate for a very long time unsupervised and they can become outdate quickly. Low power networks may be enough to send small amounts of sensor data but not a system update. This is one of the main security concerns with any computer system, and IoT has raised particular problems in terms of updating software when it becomes insecure.

Manufacturers to date have taken a lax view of security because they are rarely liable. The poor security of default passwords, for example, has led to major breaches of devices such as surveillance cameras. These functionalities in devices are in software, which is provided as a service under license, and these normally exclude all liability for damages. The lack of incentive for operators of IoT devices to deliver secure designs or fix flaws means that users and third parties are made responsible in practice. This is a major issue for the ethical design of IoT, and a recurring theme in our fieldwork.

Regulators and policy makers in Europe and elsewhere[207] are trying to solve these issues, such as security patches, but the wider issue of liability is more difficult to fix. Broader cybersecurity regulation is being advanced but tends to operate at a very high level, in practice targeting infrastructure or government networks, and offers little support to standalone IoT developers. These should certainly be aware of their new requirement under EU law, as discussed below.

At a more practical level, there are now dozens of frameworks and guidance on IoT security by various networks and bodies. Companies such as Microsoft[208] and Cisco[209] are publishing their own security policies and frameworks for IoT. Below is a summary of frameworks that may be more relevant to developers.

11.1 EU Cybersecurity Regulation

The EU and member states such as the UK and Estonia are dedicating serious resources to cybersecurity. Concerns about Russian and Chinese activities have mounted in recent years, as a general sense of distrust towards ICT sinks in, particularly since the Snowden leaks demonstrated that activities previously considered in the realm of fiction were widespread, and that supposedly secure technologies had in fact been breached to a certain extent by government hackers in the US and UK and could potentially be broken by any hostile actors.

Cybercrime, including the use of technology to steal luxury cars or perform burglaries is becoming the new norm for professional criminals. However, much like in any discussion about crime there are challenges when framing problems exclusively through this lens. Social issues can have a criminal component but do not always require a law and order solution. Conversely, reducing complex socio-technical issues to cybersecurity can lead to mass surveillance and a reduction of agency for internet users. Ultimately, this is leading to a militarisation of cyberspace of unforeseeable consequences. European cybersecurity works in practice through national structures but the European Union is trying to build common frameworks and regulations.

11.2 The NIS Directive

The Directive on security of network and information systems (the NIS Directive)[210] came into force in August 2016, with member states having until may 2018 to implement it. The directive sets out obligations for countries to maintain some cyber security infrastructure, including Computer Security Incident Response Teams (CSIRT) and a competent national Network and Information Security authority. Most EU counties already have such bodies, but in many cases they can be more focused on supporting the military and government rather than Internet of Things developers.

Special industries providing essential services such as energy, transport, healthcare, banking or ‘digital infrastructure” have special obligations. IoT can fall under this spending on the criteria of national authorities implementing the directive. These obligations include following security policies and notifying authorities of any breaches. IoT developers working on any of the essential or digital services covered by the NIS directive will need to check their national implementation for specific obligations.

One criticism from civil society is that individuals or companies affected do not have to be notified, only governments who are under no obligation to fix the problems and could even use the vulnerabilities disclosed to produce their own offensive cyber-weapons. The directive has also been criticised for not being more prescriptive on issues such as compulsory critical security updates, leaving these details to risk assessments, and not having strong penalties.[211]

11.3 ENISA Regulation and Certification

In September 2017, the European Commission published a draft proposal for a new regulation that would update the rules around ENISA.[212] The Greece-based European Union Agency for Network and Information Security (ENISA) is the centre of expertise for cyber security in Europe producing recommendations and supporting policy making. The proposals would create a new EU certification framework for information security to be recognised across all member states.[213]

A stronger role for this agency is part of the programme for a more centralised EU cybersecurity policy, but it may clash in practice with the role of national information security agencies, which will not share their utmost secrets in order to protect their work with their national spying agencies. In the UK, the information security agency is part of the spy agency GCHQ, which has been spying on EU officials in the past. ENISA has already published IoT related guidance for smart cars, airports, hospitals, and transport systems.[214]

11.4 IoT Security Foundation

The IoT Security Foundation (IoTSF)[215] is formed bykey technology players, such as Arm, Huawei, IBM and Samsung among others. Most of their activity seems to involve UK based experts.

The IoTSF is comprised of various working groups, one of which maintains a security compliance framework for a system of self-certification and another produces vulnerability disclosure guidance, which is a critical security aspect. The framework contains a checklist and questionnaire tailored for various aspects of IoT following a systematic architectural approach, such as securing cloud or device hardware. The foundation also produces simpler guidance[216] around securing data.

The foundation maintains a Best Practice User Mark system, which is free to use by anyone who complies with their guidelines, but there is no verification process and the foundation is clear that it is not a guarantee.

11.5 Cloud Security Alliance

The Cloud Security Alliance[217] is led by large industry players, such as Amazon, Microsoft, and Oracle, and includes many other high-profile members.

The alliance has produced a simple 13 step guide to securing IoT products that sets out practical measures and seems more geared towards developers than guidance that targets organisations. For example, the guidance starts by looking at development methodology, rather than data, architectural or business practices.[218]

11.6 OWASP

The Open Web Application Security Project (OWASP)[219] is a respected open non-profit organisation that provides guidance and documentation on security for web systems. Their guidance is fluid and peer produced, with most of their materials available through a wiki site.

Their IoT security guidance[220] targets the higher service and nearby networking layers – authentication, encryption, interfaces – but feels generic and not tailored to IoT. For example, their physical security recommendations look at locking down external ports such as USB, while IoT devices may have much more complex connections for actuators or sensors and locking these down may not be that simple.

11.7 BITAG

The Broadband Internet Technical Advisory Group is a consensus-based expert group that produces guidance, technical analysis, and recommendations. Its membership is more mixed than that of industry alliances, with independent academics and NGOs taking part. BITAG guidance can be useful for developers, as it makes a series of recommendations around organisational policies – vulnerability disclosures, follow best practices – but also for design requirements – e.g. function without internet connectivity or cloud back up.

The Broadband Internet Technical Advisory Group lists[221] various issues that they believe contribute to making IoT more risky than other tech areas: the general lack of supply chain experience on privacy and security affects developer and manufacturers, and, in some cases, could even mean malware is installed during fabrication. There is a lack of incentives to provide security upgrades to software, including over the air through remote management.

11.8 Online Trust Alliance

The Online Trust Alliance (OTA)[222] is an initiative within the Internet Society (ISOC),[223] one of the key non-profit groups that has been working to build an open internet for the past two decades. ISOC participates in internet governance spaces and standards driving fora, bringing a public interest perspective to some industry dominated processes. OTA focuses on building trust on the internet through promoting privacy and security, and also includes various corporate members including Microsoft.

The OTA has produced an IoT Security & Privacy Trust Framework[224] that explicitly aims to provide developers with prescriptive advice. The framework includes 12 security principles for the design of systems, guidance on user access, and extensive policies for privacy, disclosures and notifications. The latter includes IoT specific aspects such as making visible any physical tampering with devices. The security design principles seem relevant to European developers, but some of the policies are US centric and would need thorough checking to ensure they do not fall short of GDPR or European consumer legislation. This is a common problem.

11.9 ISA/IEC 62443

The International Society of Automation (ISA) is a non-profit professional body that sets standards and develops best practice in the field. It is an accredited standards developing organisation in the USA but international in scope.

The ISA99 committee[225] works on Industrial Automation and Control Systems Security, and currently includes over 500 international industrial cyber security experts. This work of ISA99 work is incorporated by the International Electrotechnical Commission in producing the multi-standard IEC 62443 series.

IEC 62443: Industrial Network and System Security[226] is a standard for industrial applications and may not be relevant for many IoT developers. For those working on SCADA systems or even some smart city settings it could be important.

11.10 Industrial Internet Consortium

The IIC as discussed above is managed by the OMG, which as discussed provides frameworks, not standards. Their framework for security[227] contains useful information for developers thinking about security but implementing its systematically is certainly overkill for independent designers.

11.11 GSMA

The GSMA security guidelines for IoT[228] are deceptively simple but could be effective. They work through a risk assessment process model, rather than a list of recommendations, architectural walkthrough, or design principles. The guidelines contain some useful case studies as examples, such as a wearable device and a drone.

[207] NTIA. (n.d.). Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching. Retrieved November 28, 2017, from https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

[208] Microsoft. (2017). Cybersecurity Policy for the Internet of Things. mscorpmedia.azureedge.net.

[209] Cisco. (n.d.). Securing the Internet of Things: A Proposed Framework. Retrieved November 28, 2017, from https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

[210] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[211] Byström, N. (2016, September 5). Cybersecurity directive not enough to protect digitising European industry. Retrieved November 28, 2017, from https://www.euractiv.com/section/digital/opinion/cybersecurity-directive-not-enough-to-protect-digitising-european-industry/

[212] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (‘’Cybersecurity Act’’)

[213] European Commission. (n.d.). The EU cybersecurity certification framework. Retrieved November 28, 2017, from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

[214] ENISA. (n.d.). IoT and Smart Infrastructures. Retrieved November 28, 2017, from https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures

[215] IoT Security Foundation. (n.d.). ESTABLISHING PRINCIPLES FOR INTERNET OF THINGS SECURITY. Retrieved November 28, 2017, from https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf

[216] ibid.

[217] Cloud Security Alliance. (n.d.). Home – Cloud Security Alliance. Retrieved November 28, 2017, from https://cloudsecurityalliance.org/

[218] Cloud Security Alliance. (2016). *Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products.* downloads.cloudsecurityalliance.org.v

[219] OWASP. (n.d.). About The Open Web Application Security Project. Retrieved November 28, 2017, from https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

[220] OWASP. (n.d.). IoT Security Guidance. Retrieved November 28, 2017, from https://www.owasp.org/index.php/IoT_Security_Guidance

[221] Broadband Internet Technical Advisory Group. (2016). *BITAG Report – Internet of Things (IoT) Security and Privacy Recommendations*. bitag.org.

[222] Online Trust Alliance. (n.d.). Online Trust Alliance. Retrieved November 28, 2017, from https://otalliance.org/

[223] Internet Society. (n.d.). Home | Internet Society. Retrieved November 28, 2017, from https://www.internetsociety.org/

[224] Online Trust Alliance. (2017). IoT Security & Privacy Trust Framework v2.5. otalliance.org.

[225] ISA99 Committee. (n.d.). ISA99: Developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS). Retrieved November 28, 2017, from http://isa99.isa.org/ISA99%20Wiki/Home.aspx

[226] ISA. (n.d.). The 62443 series of standards. Retrieved November 28, 2017, from https://scadahacker.com/library/Documents/Standards/ISA%20-%2062443%20Series%20Overview.pdf

[227] Industrial Internet Consortium. (2016). *Industrial Internet of Things Volume G4: Security Framework IIC:PUB:G4:V1.0:PB:20160926.* iiconsortium.org.

[228] GSMA. (2016).*v* gsma.com.

12. Conclusion

While IoT may not be regulated as such, IoT products placed in the market are covered by various laws and standards. Developers may not be generally aware of the complexity of electromagnetic and telecoms regulations. The regulations we have covered in this section are the result of policies that embody diverse social concerns about safety, fair competition, the environment and the health of consumers and workers, among others. These concerns extend to ethical considerations.

In discussions about data protection and privacy, we do not expect strict legal compliance to be the only expectation. Similarly, when it comes to other ethical issues, developers will face the question of whether to comply with the law, or take a stronger ethical stance.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732027

This report is the result of H2020 project VIRT-EU:

virt•eu OPEN RIGHTS GROUP