Project no. 732027

VIRT-EU

Values and ethics in Innovation for Responsible Technology in EUrope

Horizon 2020

ICT-35-2016
Enabling responsible ICT-related research and innovation
Start date: 1 January 2017 – Duration: 36 months

Deliverable 2.2

Due date: 30 Novemeber 2017

Actual submission date: 1 December 2017

Number of pages:

Lead beneficiary: London School of Economics and Political Science

Author(s): Alison Powell, Selena Nemorin, Annelie Berner, Rachel Douglas-Jones, Ester Fritsch, Obaida Hanteer, Matteo Magnani, Alessandro Mantelero, Luca Rossi, Javier Ruiz, Irina Shklovski, Shaira Thobani, Davide Vega-Aurelio,

Project Consortium

Beneficiary no.	Beneficiary name	Short name
1 (Coordinator)	IT University of Copenhagen	ITU
2	London School of Economics	LSE
3	Uppsala Universitet	UU
4	Politecnico Di Torino	POLITO
5	Copenhagen Institute of Interaction Design	CIID
6	Open Rights Group	ORG

Dissemination Level

PU	Public	**X**
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	

Dissemination Type

R	Document, report	**x**
DEM	Demonstrator, pilot, prototype	
DEC	Websites, patent filling, videos, etc.	
O	Other	
ETHICS	Ethics requirement	

Executive Summary

The networked future promises new relationships between people and artifacts, the private and the public, the individual and the collective. Recent policy, such as the EU General Data Protection Regulation, reflects mounting public concerns around emerging data practices, responsible research and innovation (RRI), data ethics and privacy. VIRT-EU seeks to address these concerns at the point of design through researching and intervening upon the development cultures and ethics of the next-generation IoT innovators. We ask how do European IoT innovators and developers make ethically consequential decisions – about code, hardware and data – for new connective devices? What assumptions about human behavior, privacy and freedom underpin European cultures of IoT innovation?

Goals
VIRT-EU aims to analyze and map the ethical practices of European hardware and software entrepreneurs in order to:

- Understand how Internet of Things (IoT) innovators enact ethics as they design future devices;
- Generate a new framework for Privacy, Ethical and Social Impact Assessment (PESIA); and
- Develop tools to support ethical reflection and self-assessment as part the design and development process for IoT technologies.

The project concentrates on developing and applying ethical frameworks, which requires a strongly integrated interdisciplinary approach that is able to describe and analyse social processes of ethical thinking and acting, social relationships, and a set of frameworks for action and reflection. As such, the project is comprised of qualitative, quantitative, legal, and design approaches. This report presents outcomes of the substantive research and interdisciplinary synthesis of findings produced during the first year of empirical and theoretical development of the Virt-EU research project on values and ethics in innovation for responsible technology in Europe.

Focus and Methods
The focus of our initial work has been twofold. First, we engaged in an inter-disciplinary mapping of where, how, and with what consequences designers, developers, thinkers and practitioners talk about ethics in relation to the IoT, including network analysis and qualitative domain mapping. Second, we conducted an extensive overview of the current legal and regulatory landscape that affects development, commercial production, and use of IoT devices and services.

The use of online digital data and social network analysis tools developed by UU and ITU has guided qualitative exploration into new sites of observations and complemented insights obtained through qualitative analysis. Online data constitute an important resource throughout the project.

Through fieldwork in London, Geneva, Lyon, Torino, Copenhagen, Bled, Malmö, Berlin, and Barcelona our LSE and ITU project teams were able to map the most commonly expressed ethical values and reflect upon how these values were discussed and instantiated. This initial exploration allowed us to empirically derive locations for in-depth focused research in the coming year, based on indications of IoT innovation and investment in particular locations, especially London and Amsterdam, due to clustered research, civic innovation, and SME industrial contexts

This first empirical exercise comprised ethnographic methods such as observations, extended field notes, interviews, and document and policy analyses have been used thus far to make sense of emerging data practices, responsible research and innovation (RRI), and data ethics at the point of design in relation to the Internet of Things. Alongside these exchanges, formally planned, semi-structured interviews were conducted with a range of IoT community participants. Observational research included a mix of both non-participatory observations and participation in certain events such as policy development working groups and presenting papers at conferences.

A second empirical exercise comprised a document analysis which showed that over the last several years there has been a proliferation of public statements, manifestos, and calls from advocates, designers, and developers for negotiating alternative or oppositional positions for the IoT, often specifically referring to ethics (or values in general). Emerging from a sense of uncertainty, these manifestos create publics for debate, demand attention and call for change.

Working toward the development of a Privacy, Ethical and Social Impact Assessment (PESIA) framework, project partners Polytechnic University of Turin (POLITO) and Open Rights Group (ORG) have conducted initial research on policies and institutional contexts for data identification, collection and analysis in Europe.

Our process for integrating research has been based on collaborations across interdisciplinary teams. Towards the end of the WP2 work cycle we conducted an all-consortium synthesis workshop coordinated by CIID, presenting findings from each team and working together to develop new research questions and interdisciplinary approaches. The ITU-based *Data Sprint* brought the qualitative and quantitative teams

physically together to explore and experiment with a selection of data collected. The primary objectives were familiarisation and synthesis of research approaches, with a view to producing better understandings of one another's research processes and requirements across teams.

Initial Findings
Our initial research findings show that:

- IoT developers lack practical guidance on the ethical and social issues of data use. Moral reasoning and ethical conduct are rarely topics for discussion online or offline in communities of IoT developers and innovators, even though they have an implicit ethical framework of some kind.
- Discussions about IoT online do not emerge in relation to specific locations; rather conversations among a core group of people continue across different events
- Some of the most commonly encountered ways of discussing ethical issues are in relation to privacy and trust, security, data management, responsibility, and openness and interoperability. IoT in personalised sensing is also understood in relation to wellness and care.
- IoT developers negotiate these ways of engaging with ethical issues relationally, but also develop oppositional perspectives as evident in the production of IoT manifestos
- Virtue ethics provides an important framework in which dialogue about information technology ethics can occur.
- Law, regulation, and manufacturing contexts nuance how people talk about values.
- Conflicts emerge between how IoT developers and citizens perceive issues of personal data, suggesting that new soft law frameworks are required
- Key standards and regulations shape the way that IoT devices operate, are integrated into workplace practices, and consequently respond to legal and social contexts
- Continued interdisciplinary research synthesising these different disciplinary approaches is required for
    - Identifying further situated research cases
    - Identifying specific elements necessary for the development of a PESIA
    - Linking network analysis, qualitative research and legal and policy scholarship
    - Mobilizing communities of practice for participation in the development of PESIA

1.0 Introduction

This report presents outcomes of the substantive research and interdisciplinary synthesis of findings produced as part of the work conducted for Work Package 2. The major goals of this work package were first, to develop methodological infrastructures and practices to support highly interdisciplinary work, and, second, to conduct an in-depth domain analysis that will lay the groundwork for in-depth field engagements, theory development and tool prototyping planned for the next two years.

Methodologically, in order for the VIRT-EU project to achieve its overall goals, it was crucial that we collaboratively establish mechanisms to ensure the successful integration of theoretical development with the results of the qualitative, quantitative, and legal research activities, and develop interdisciplinary practices that can support this. We achieved this by developing custom software and interfaces that enabled qualitative and quantitative researchers to make decisions about data collection and to collaboratively engage in data analysis that lead to mutually beneficial insights. We also worked to establish consistent channels of communication between the qualitative researchers and the legal scholars in order to develop practices that would allow us to enrich legal approaches with qualitative empirical content and vice-versa. Finally, we conducted a successful research synthesis workshop that involved the full consortium and allowed us to fruitfully engage with our diverse Advisory Board.

Substantively, the focus of our initial work has been twofold. First, we engaged in an inter-disciplinary mapping of where, how, and with what consequences designers, developers, makers, thinkers and practitioners talk about ethics in relation to the Internet of Things. Second, we conducted an extensive overview of the current legal and regulatory landscape that affects development, commercial production and use of IoT devices and services. To accomplish this we used network modeling of discussion networks where issues of ethics emerge and circulate; qualitative domain mapping including observations made at events across Europe, interviews, and analysis of written materials; and legal and policy scholarship covering ethical aspects of policy decision making. This deliverable reports on the outcome of these activities as well as on the synthesis and connection between these three areas.

The content of this deliverable is organised as follows. We begin with an overview of relevant discussions of IoT and ethics across the law, sociology, communication studies, and design literature, highlighting the particular problems that IoT technologies specifically bring forward and identifying potential avenues of addressing these problems through research and design approaches. We then detail empirical efforts to identify and contextualise the empirical domain for the application of quantitative

network analysis and ethnographic investigations as well as opportunities for intermixing these approaches. We continue by summarizing initial research on policies and institutional contexts for data identification, collection and analysis in Europe combined with an overview of the regulation and standards affecting aspects of the IoT other than data protection in the EU. We conclude by identifying further strategies for our project work over the next period – the results-based integration of online networked data into the process for identification of future field sites, the synthesis between sociotechnical analysis of technology and ethics and the review of soft law and policy, and the use of parallel research strategies across disciplines. In this way we ensure the integration of multiple methods across the project.

1.1 Relevant Scholarly Discussions of IoT

Although Internet-connected appliances of various kinds have occasionally been developed since the 1980s, starting with the Coca-Cola machine at Carnegie Mellon University in 1982, the term 'Internet of Things' was originally coined by Kevin Ashton in '99 in an effort to describe the potential of RFID tags and the Internet for modernising large-scale supply chains at Proctor & Gamble. Since then the use of the term has expanded to encompass a dizzying variety of connected devices and services to the point where defining what precisely does and does not qualify as IoT is neither particularly simple nor useful any longer. One of the goals of the VIRT-EU project has been to investigate from a grounded perspective the significance of ethical issues in the design of products and services that their developers term IoT. Our exploration of the domain has differed from the standard modes of describing the rise of the IoT in relation to numbers of connected objects[1] or to the arbitrary description of 'sectors' in which Internet-enabled devices might be employed. Instead, we see the development of the IoT as an occasion to examine longstanding issues of information policy in design, as well as persistent ethical issues that grows in complexity as IoT development gains momentum.

1.2 IoT Opportunities and Challenges

The notion that technologies are not neutral forms is one of the core assumptions of the constructivist tradition in science and technology[2] and the ethics of the design of new

[1] Thibodeaux, T. (April 28, 2017). Smart cities are going to be a security nightmare. *Harvard Business Review*. Retrieved from http://bit.ly/2oQv9q4; Cisco. (2011). Securing the Internet of Things: A Proposed Framework. Retrieved from http://bit.ly/2zpBpeN

[2] Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice*, *5*(4), 379-393; Pinch, T. J, & Bijker, W. E. (1984). The social construction of facts and artifacts: Or how the sociology of science and the sociology of technology might benefit each other,' *Social Studies of Science, 14*(3), 399-441; Winner, L. (1980). Do Artifacts have politics?' *Daedalus*, 109, 121-136;

technologies has been part of the 'values in design' movement since the 1980s[3]. Therefore, some of the considerations of the ethics of emerging IoT are continuous with past concerns about values, while others resurface and recombine thorny issues in code and law: issues of data sharing, use and ownership, agency and autonomy of systems and the people who use or benefit from them, issues of discrimination resulting from the extensive collection of data, and the increasing role of technological design as a legal and policy actor.

Discussions of IoT and its potential encompass positive expectations and cautionary concerns among scholars. Some have claimed that connected products and the data they can generate will usher in an era of competition that should not be impeded by over-regulation. In this view, the IoT will alter the structure of industry not only through reshaping industry boundaries but also by creating new industries. These changes, however, are exposing companies to both competitive opportunities and threats. Porter and Heppelman[4], for example, see IoT as an opportunity to drive rapid innovation and economic growth, accompanied by prosperity. In light of these developments, industry and government have a social, economic, and ethical imperative to equip workers with the skills to participate in this new competitive environment, and to create rules and regulations for setting standards, enabling innovation, protecting data, and overcoming efforts to block progress.

Cyberlaw and social studies of connected systems stress the complexity of connected systems. In the cyberlaw field, Matwyshyn[5] explores ethics and values in terms of the relationship between IoT and consumer law. She claims that as technology services in governmental and private sectors increasingly move to the "cloud", questions of consumer privacy have become more urgent, yet there remains uncertainty in the field of consumer privacy law. Matwyshyn's concerns with whether consumers hold any legally protectable interest in their data after collection resonate with Edwards' (2015) concern about sensor-based data use across European 'smart cities' projects and the impossibility of achieving prior consent to data use in these cases. She identifies three possible routes forward: (i) exploring the development of a holistic privacy impact assessment (PIA) for smart city data flows; (ii) finding new means for obtaining some kind of standing or "sticky" consent to data processing decoupled in time from when the

[3] Shilton, K. & Koepfler, J. A. (2013). Making space for values: communication & values levers in a virtual team. *Proceedings of the 6th International Conference on Communities and Technologies* (Munich, Germany), 110-119; Knobel, C.P. & Bowker, G.C. (2011). Values in design. *Communications of the ACM 54*, 26–28; Friedman, B., Kahn, P.H., & Borning, A. (2006). Value sensitive design and information systems. In D. Galletta and P. Zhang, eds., *Human-Computer Interaction and Management Information Systems: Applications*. M.E. Sharpe, New York.

[4] Porter M. E. & Heppelmann, J. E. (2014) How smart, connected products are transforming competition. *Harvard Business Review, 92*,11–64.

[5] Matwyshyn, A. M. (2013). Privacy, the hacker way. *Southern California Law Review*, *87*(1), 1-68.

data is actually pervasively collected via the IoT; (iii) implementing a legal right to algorithmic transparency and finding ways of making this knowledge useful to ordinary users."[6].

The temporal issues of data collection that are part of the IoT include longstanding issues of liability that might cover who is responsible for inaccurate data or failure to attain proper anonymisation of the data collected[7], but also new issues that Hildebrandt suggests might represent the 'ends of law'[8]. Such 'ends' include the inability for existing legal frameworks (in soft or hard law) to address the ethical challenges of data sharing, as well as the increased role of design in addressing ethical issues. While Hildebrandt and Edwards might be cautiously optimistic about the role of design or ethical impact assessment, they also acknowledge that these decisions are taken in the context of highly competitive market environments combined with a 'regulatory entrepreneurship' where some technology companies use political power to secure regulatory frameworks that are of economic benefit to them rather than broadly socially valuable[9].

New technologies also pose challenges as they can develop features in advance of specifically targeted policy or regulation. In technological design this 'disruption' is often positioned as if it were positive, since it can generate financial benefit. However, it also raises both regulatory questions and serious issues related to power and influence. Who owns the data these sensors generate? How can such data be used? Are these devices, and the data they produce, secure? And are consumers aware of the legal implications that these data create—such as the possible use of data by an adversary in court, an insurance company when denying a claim, an employer determining whether to hire, or a bank extending credit?[10]. Peppet also examines how various dimensions of sensor-based technologies create discrimination (including racial or protected class discrimination and economic discrimination); privacy; security; and issues with consent.

Sensor data collected through IoT applications can also potentially be used in remote contexts to make decisions about insurance, employment, credit, housing, or other sensitive economic issues, in contexts that reiterate the privacy and security

[6] Edwards, L. (2015) Privacy, security and data protection in smart cities: a critical EU law perspective. Retrieved from http://ssrn.com/abstract=2711290
[7] Maughan, A. (July 5, 2014). The Internet of Things: A lawyer's guide. *Society for Computers & Law*. Retrieved from http://www.scl.org/site.aspx?i=ed37862
[8] Hildebrandt, M. (2015). *Smart Technologies and the End(s) of Law*. Northampton, MA: Edward Elgar.
[9] Pollman, E. & Barry, J. M. (2017). Regulatory entrepreneurship. Southern California Law Review, *90*, 383-448.
[10] Peppet, S. (2014). Regulating the Internet of Things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review*, *93*(1), 85-176.

implications attached to the processing of data about marginalised people[11] including the processing of unstructured 'big data' of the sort that IoT sensors provide. Even when anonymised, this kind of big data processing can have disparate impact on marginalised communities[12]. Because of the nature of big data processing which is often based on machine learning techniques, existing frameworks for privacy and data security may be unable to address long-term risks related to reproduction of bias through data processing.

1.3 The Ethical Turn

The legal, policy and equity challenges raised in relation to IoT has inspired research that takes an explicit ethical perspective, such as Lupton's[13] reflection on how selfhood, embodiment, and social relations have increasingly become developed via digital technologies. Lupton identifies that a consequence of this is that 'algorithmic authority' is exerted, in which decisions made by software developers play a significant role in shaping individuals' life chances. In addition, the structural arrangements that underpin these data processes are a concern for political economists: Mosco[14] is concerned with the relationship between IoT, cloud storage, and data protection, because "it entails moving all data from relatively well-known settings where the home computer hard drive is under personal control or the computer at work stores data behind an employee's firewall at an on-site data center" (p. 141). He argues that the storage of large amounts of personal information in the cloud opens this data to malicious attacks given the multi-layered processes implicated in the systems designed to store and protect such data. Significant ethical issues arise as a result of these digital moves, including privacy threats related to revenue streams flowing from consumers' own personal data.

Along similar lines, surveillance studies scholars, Andrejevic and Burdon[15], argue that forms of pervasive, always-on, passive information collection are beginning to characterise the use of digital devices and the business models with which they are associated. To make sense of the significance and implications of these social developments, the authors propose the concept of the "sensor society". The term refers to a world of processes of data collection and use that reconfigure privacy, surveillance, and sense-making. In this kind of environment, certain groups and individuals hold data mining privileges that may not benefit society more broadly.

---

[11] Gangadharan, S. P. (2017). The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal Internet users. *New Media & Society*, *19* (4), 597-615.
[12] Barocas, S. & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, *104*(3), 671-732.
[13] Lupton. D. (2016). The diverse domains of quantified selves: self-tracking modes and dataveillance. *Economy and Society, 45*(1), 101-122.
[14] Mosco, V. (2014). *To the Cloud: Big Data in a Turbulent World*. Boulder, CO: Paradigm.
[15] Andrejevic, M. & Burdon, M. (2016). Defining the sensor society. *Television & New Media, 16*(1) 19–36.

From an economics and public administration perspective, Popescul and Georgescu[16] explore the ethical implications of IoT that emerge as a result of data transfer from virtual to physical devices. They argue that information transfer is exacerbated by the extended use of new technologies such as RFID, NFC, sensors, 3G and 4G, which not only transfer traditional information security threats to the IoT environment but also create new threats. Their overview of the ethical landscape is prompted by an important question asked by European Commissioner, Gerald Santucci[17], Head of *Internet of Things and Future Internet Enterprise Systems Unit*: What place will human beings have in a world in which 7 billion people live together with 70 billion cars and a few thousand billion objects connected to an infrastructure of global networking, having the ability of self-coordination, self-configuration and self-diagnosis?

1.4 Responses to IoT Ethical Issues

Different perspectives on how to respond to these ethical issues have been proposed by researchers across disciplines. Where Howard[18] suggests that an industry-led "Pax Technica" based on common technological standards and a worldwide network of devices can create political stability at a global scale, he is suggesting that one of the points of recourse to unethical IoT is to have connected devices dedicate a portion of their processing power/time to an activity that would benefit the common good. The questions that emerge here, then, are both moral and political: In the increasing proliferation of IoT and mass amounts of data collection/circulation, apart from privacy what else might be considered a common good? Who decides what this common good is? Who should decide how it can best be served? Also, how do the instruments of measurement, collection, and dissemination shape culture/s and discourse?

Popescul and Georgescu[19] claim that ethical behaviour in regards to information communications technology more broadly hinges on the enforcement of property rights on information; ensuring user access to information; maintaining integrity of information; and enforcing the right to private life, suggesting the significance of legal and democratic frameworks to delineate the limits of this communicative practice must be put into place.

---

[16] Popescul, D., & Georgescu, M. (2013). The Internet of Things – Some ethical issues. *The USV Annals of Economics and Public Administration,* 13 (2/18), 208-214.
[17] Santucci, G. (4, Feb, 2011), The Internet of Things: A Window to Our Future. Retrieved from http://bit.ly/2hvKnzy
[18] Howard, P. N. (2015). *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. Austin, TX: Yale University Press.
[19] Popescul, D., & Georgescu, M. (2013). The Internet of Things – Some ethical issues. The USV Annals of Economics and Public Administration, 13 (2/18), 208-214.

This review of the literature identifies that while many of the broad legal, sociological and political-economic issues connected with the development of IoT devices are in continuity with long standing discussions about ethical risks of expanded access to communication technologies, IoT technologies specifically bring forward problems with the ‘ends of law’ - where development of data sharing economies outpace hard or even soft regulatory frameworks, and suggest the necessity for addressing ethical issues through design. Furthermore, the review of the literature suggests that ethical issues vary according to contexts, and don’t necessarily align with divisions based on application sectors.

The next sections illustrate how we might understand some of these ethical issues, drawing from network analysis, qualitative domain mapping, a review of legal and soft law issues as well as regulations and standards that impact on the development of IoT tools. Following, our consortium describes how we synthesize different forms of knowledge in order to deepen our understanding of these issues.

2.0 Network Analysis: Using Online Digital Data

The use of online digital data can guide qualitative exploration into new sites of observations and complement insights obtained through qualitative analysis. There are two reasons why an integrated approach to data collection is preferable. First, while participation in IoT related events, ethnographic analysis and interviews provide very rich data, they are costly and time consuming methods. On the other hand, the monitoring of IoT-related online discussions is cheap, efficient and can collect data for several simultaneous events, although the quality of the insight obtained with these data is often poor. Second, while ethnography needs a specific filedsite clearly defined both in temporal and spatial terms, online data collection can run for an undefined period of time and potentially capture the dispersed conversations that are happening online across time and geography.

As a general note we acknowledge that both types of data are biased toward the context where they are collected, however putting them together may reduce the overall bias. Recommendations regarding relevant events, actors or topics, may emerge from the analysis of a large amount of online data, so that ethnographic analysis can be focused. At the same time, ethnographic analysis will continue to give rise to particular questions that can be productively asked of quantitative data as well as identify emergent quantitative data sources that are more community and/or topic specific and could be productively mined.

Thus online data constitute an important resource throughout the project and are used to accomplish three main objectives:

1. Provide an inclusive mapping of online platforms where issues of ethics emerge and circulate.
2. Help identify participants for workshops organised by the Virt-EU consortium for co-design and stakeholder engagement activities. The choice of participants will be based on the combination of information derived from ethnographic engagements as well as from the structure of the network of online interactions, such as identifying central individuals from different online communities that do not currently interact (Tasks 2.1; 2.2).
3. Explore to what extent project activities influence the on-going discussion about IoT and ethics. This is the most ambitious objective. However, if this is the case, we should be able to observe changes over time in the network data representing online interactions.

In the rest of this section we detail the steps we have taken to date to achieve the above goals. We first detail the selection of data sources and methodological decisions necessary for making the data available to the whole research team for joint analysis. We then describe the software tools we have developed to enable interdisciplinary engagement. Finally, we report on the preliminary network analysis performed on the initial data.

2.1 Mapping Networks of Discussion

Online discussion networks are potential key sources of data about conversations, key actors and the language they use, relationships and locations of dense or significant activity. For these reasons we explored a large number of potential data sources that could be used productively, eventually focusing on: (1) Twitter data, (2) MeetUp data, (3) LinkedIn data, (4) other specific and mostly static websites, such as the site of the Internet of Things Council. These platforms were identified through a combination of preliminary data mining and ethnographic exploration of the fieldsites of London and Barcelona that were pre-selected during the proposal stage. Although our initial expectations were to locate specific online locales where IoT developers congregate and discuss issues specific to these communities, we quickly found that the IoT space is quite immature and does not have obvious online venues for dedicated discussion. In fact, the field is quite dispersed to much frustration of the developers themselves. Two data sources immediately emerged as central for "keeping up" with the happenings in this area – Twitter and MeetUp. LinkedIn appeared to be an important way for IoT developers to self-identify as working within the IoT area, while smaller static websites signaled allegiance to one or another discussion community.

After a deeper analysis of the technical feasibility and of the use of these data sources by the community of IoT developers, we made the decision to remove LinkedIn from the list of data sources. This is due to both the mostly static nature of LinkedIn– largely used as a repository for potential collaborations and hiring opportunities rather than for actual discussions – as well as due to the difficulties in accessing the data through an API-based approach.

2.2 Online Data Collection: Tool Development and Methodological Challenges

The development of tools for collection of online data to support the different parts of the project formed a large part of the activities planned for the first year (Task 2.1). We expect the data collection to continue until the end of the project, thus the set-up of the technical infrastructure was required and largely concentrated in the first ten months of activity. The digital data collection planned for VIRT-EU presented a number of challenges that are common for researchers dealing with online social media data[20]. In addition to these general challenges, the multi-platform design of the VIRT-EU data collection confronted the researchers with new and unprecedented problems: a) data accessibility & API; b) multi-platform user mapping; c) data ephemerality and storage.

2.2.1 Data Accessibility and API

Digital data in usually collected through two major approaches. Data can be scraped from online web-sites through ad-hoc scrapers realised by the research team or data can be obtained through official APIs made available by the digital platform we want to

[20] Giglietto, F., Rossi, L., & Bennato, D. (2012). The open laboratory: Limits and possibilities of using Facebook, Twitter, and YouTube as a research data source. *Journal of Technology in Human Services*, *30* (3-4), 145-159.

study. While an evaluation should be done case-by-case, data scraping is usually less reliable than data obtained through APIs[21].

Any specific set of API gives the researchers not only a set of actions that are actually possible but also a relatively clear framework to use the data that is defined by the platform specific terms of services. While APIs undoubtedly facilitate access to social media data they also limit and define what is accessible and what it is not, ultimately defining what can be used as research data and what cannot. This radically reshapes the whole research process by requiring researchers to develop their research questions on the basis of what data can be acquired through platform-specific APIs rather than on the basis of what would be the ideal data. Moreover APIs can change over time, new limitations (such as the number of queries allowed every second) can be introduced or the platform can decide to transform part of the entire API into a commercial service requiring a fee to be paid in order to access it. This dynamic introduces an unprecedented level of uncertainty about social media data where research design is now necessarily developed within the constraints created by platforms' API. Such a scenario is common to a large set of research activities within the context of social media.

From the outset, VIRT-EU was a carefully designed research project, which already took into consideration the major limitations, thus reducing the need to adjust our original research design as we began empirical data collection. The only limitation we have encountered was the lack of publicly available APIs for LinkedIn[22] and significant issues of obtaining access to these APIs by legal means through available direct request mechanisms. We thus reassessed the potential usefulness of the LinkedIn data in light of the costs of attempting to obtain it further and made the decision to remove this resources as a data source in the project at this time.

2.2.2 Multi-Platform User Mapping

Given the specific multi-layer approach used within VIRT-EU social media network analysis, a major challenge was the need to map the various users between different social media platforms. Due to the platform-specific nature of social media APIs, as well as local practices adopted within each platform, collecting data about a user from a specific platform (e.g. a user profile on Twitter) does not necessarily help with identifying the same user on a different platform. While this problem is largely ignored by traditional network analysis, that mostly operates within the boundaries defined by a single platform, it becomes central within a multi-layer perspective such as the one proposed by the project.

[21] Lomborg, S., & Bechmann, A. (2014). Using APIs for data collection on social media. *The Information Society*, *30* (4), 256-265.
[22] Russell, M. A. (2013). *Mining the Social Web: Data Mining Facebook, Twitter, LinkedIn, Google+, GitHub, and More*. Farnham, UK: O'Reilly Media.

The state of the art of users mapping is still in a very early stage of development[23] and while few automatic approaches have been proposed, the specificity of the user mapping requested by the VIRT-EU project required a combination of a quantitative and qualitative approach. This is why, beside the tools developed to collect and explore social media data from various platforms, a specific mapping tool has been developed. Using this tool the researchers can select specific users and map them across several social media platforms. In this way, given the limitations of the various platforms, we can obtain a multi-platform profile of every key user within the network of IoT developers. While the procedure is undoubtedly time consuming and resource intensive, it assures a high data quality.

2.2.3 Data Ephemerality and Completeness

The problem of data ephemerality is usually connected with specific social media (e.g. Snapchat) that propose ephemeral messages and communication that will not be saved either by the users involved or by the social media platform itself. Nevertheless data ephemerality can be considered, to various degrees, a common problem to every single social media platform when it is used for scientific research. Social media platforms are, almost by definition, unstable: terms of service, APIs, are always evolving, users are constantly curating the content they have produced, and platforms' moderation is always in place. These elements create a general uncertainty about the temporal persistence of data[24].

The only solution to this problem is to create local copies of the data, relying on an ad-hoc infrastructure that, rather than executing specific queries every time, stores locally the data deemed to be relevant. Obviously this approach faces the limitations posed by the APIs in terms of the quantity of data that is actually collectable (as in the case of Twitter, see Morstatter, Pfeffer, Liu, & Carley[25]) or in terms of the time required to collect the data due to how many queries are executable within a window of time. While this represents a known issue that is hard to quantify exactly, the technical solutions of the developed platform, as well as the average amount of data generated by the events under analysis, suggest consideration of its impact on the coverage of project data as negligible.

2.3 Data Collection Tools

As part of the activity of WP2.1 we have developed a suite of online tools to support (1) the automated collection of data from online sources, (2) the exploratory analysis of the collected data, (3) the manual input of consolidated data, and (4) the off-line analysis of the collected data.

---

[23] Dickison, M. E., Magnani, M., & Rossi, L. (2016). *Multilayer Social Networks*. Cambridge, UK: Cambridge University Press.

[24] Hogan, B., & Quan-Haase, A. (2010). Persistence and change in social media. *Bulletin of Science, Technology & Society, 30* (5), 309-315.

[25] Morstatter, F., Pfeffer, J., Liu, H., & Carley, K. M. (2013, June). Is the Sample Good Enough? Comparing Data from Twitter's Streaming API with Twitter's Firehose. In *ICWSM*.

The tools that are part of the first three tasks have mostly been developed specifically for the project, with the exception of the tool to collect tweets that was produced by extending existing software. These tools are intended to be used by project members from different units, and thus to facilitate interactions between the qualitative and quantitative aspects of data analysis. The fourth task - the off-line analysis of the collected data - is instead performed using an existing software library developed at the Uppsala site, extended with additional functionality required to handle the collected datasets.

2.3.1 Automated Online Data Collection Tools

As detailed in section 2.1.1 the two online platforms we are constantly monitoring for updates are Twitter and MeetUp. In both cases, a main requirement has been to allow all project members to be able to start the monitoring of different online data of interest.

For Twitter, events or online themes of discussion are often associated with specific hashtags, that can be seen as keywords that Twitter users include in their posts to indicate the context of the message. As an example, people writing tweets about the London Tech Week festival would often use the hashtag #LTW. Therefore, we have modified and deployed on our server the open source tool YourTwapperKeeper (https://github.com/540co/yourTwapperKeeper) that allows registered users to collect tweets containing a list of given hashtags. Project members can login to a web page where they can include more hashtags and inspect the current results of the other active data collection processes.

Archive ID	Keyword / Hashtag	Description	Tags	Screen Name	Count	Create Time
1	#iot	Test IoT hashtag	test	dvladek	6889562	Wed, 03 May 2017 16:44:21 +0000
14	#BornHack	Bornhack 2017 - Danish maker/hacker event	Denmark, data ethics, hacking	quillis	673	Mon, 21 Aug 2017 13:50:59 +0000
3	#iotconf17	#iotconf17	#iotconf17	LR	296	Tue, 23 May 2017 12:56:25 +0000
4	#IoTWeek2017	Geneva IoT Week	#IoTWeek2017	digiteracy	2515	Mon, 05 Jun 2017 16:43:57 +0000
5	#GIoTS2017	Geneva IoT Week	#GIoTS2017	digiteracy	234	Mon, 05 Jun 2017 16:50:37 +0000
7	#TechXLR8	IoT Conference - London	London, IoT	digiteracy	7590	Sun, 11 Jun 2017 10:30:54 +0000
8	#LTW	Tech Conference, London	#LTW	digiteracy	30701	Sun, 11 Jun 2017 10:31:35 +0000

Figure 1: Interface of the Twitter data collection tool

For MeetUp, the process is different. We have implemented a monitoring system where group members can register their MeetUp accounts (or special accounts they created for Virt-EU). Once the accounts are registered, it is sufficient for project members to join the groups and events they are interested in directly on the MeetUp website. A monitoring process is automatically started at regular intervals on our server and collects the information about all the new groups and events project members have joined.

2.3.2 Exploratory Analysis

The objective of the online exploratory analysis system for Twitter, specifically developed for this project, is to allow an interactive analysis of the collected datasets so that all project members can (1) explore the online discussion and compare it with on-site observations, (2) identify central actors in the online discussion, including actors who had not been identified through the physical participation in the corresponding event, (3) explore related hashtags and the corresponding topics of discussion, and (4) get a visual intuition regarding the structure of the conversation, in particular the presence of well-separated communities and other central actors.

All the Twitter datasets collected through the tool mentioned in the previous section are automatically made available on our analysis web site, which can be accessed only by project members. Each Twitter dataset can be explore in a number of ways. Tweets can be read and filtered according to various parameters (e.g. the presence of a specific keyword, or the author of the meesage) allowing a qualitative exploration. All datasets, both the original and those obtained applying filters, can be downloaded for further analysis with external tools.

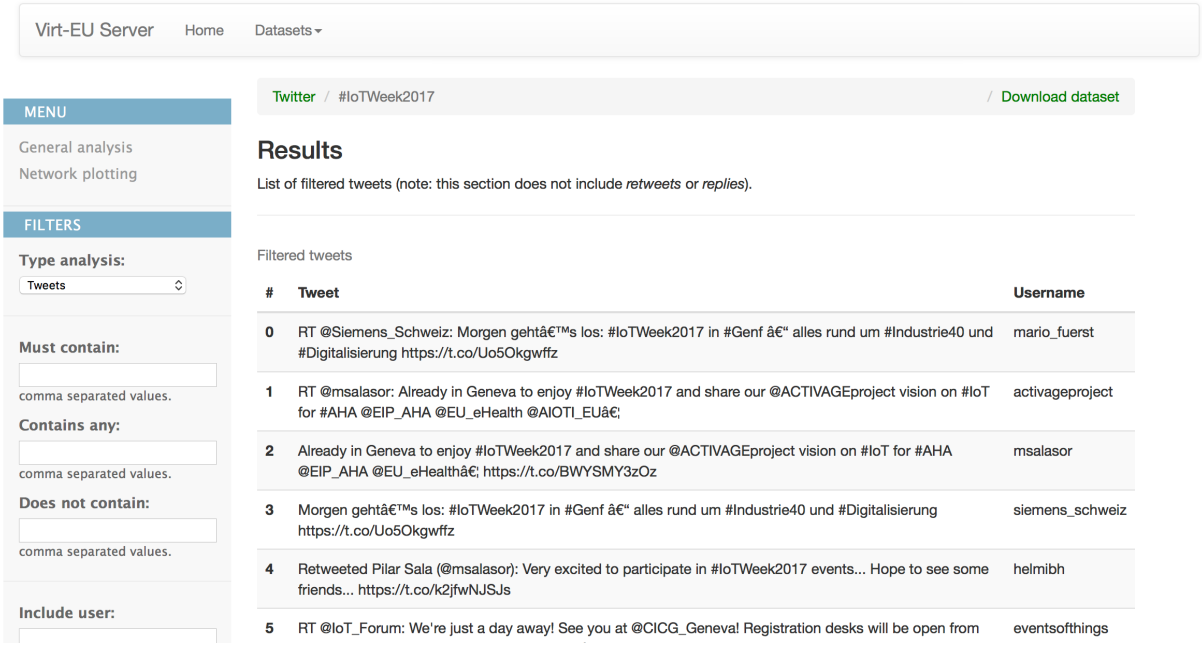

Figure 2: Interface for the qualitative exploration of the tweets.

Moreover, the researchers working with the data can have a more quantitative overview of the content of the datasets through tools such as frequency ranking of hashtags and co-occurrence analysis. Finally, for datasets of limited size it is possible to generate an interactive visualisation to reveal the structure of the network and highlight the connectivity of specific actors, that can be selected directly from the visualised graph.

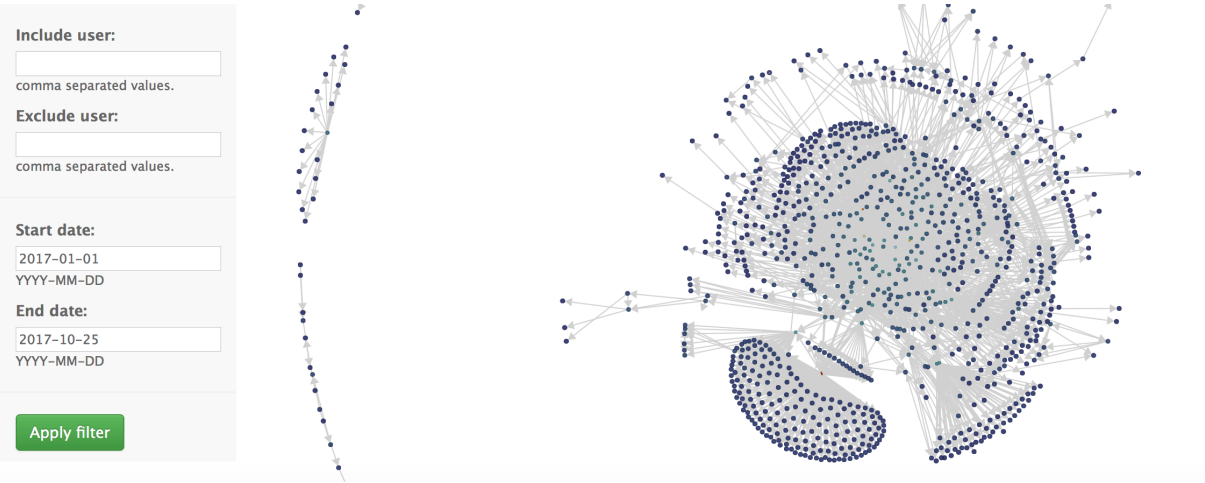

Figure 3: Example of network visualisation of the conversations present within a Twitter dataset

2.3.3 Consolidated Data for Multi-Platform Analysis

The tool for data consolidation is essential to allow the multi-platform analysis planned by the project. It is also essential to allow cooperation across research units and to guarantee high data quality. The main concepts behind this tool are that (1) data from different sources should be integrated and stored in a common format, to allow their joint analysis, and (2) only relevant and high-quality data should be part of the analysis. For example, an actor who is influential in the IoT area can be identified because she is mentioned during the interviews or because of her role in the discussion on Twitter, or because of the events she organizes on MeetUp. Therefore, we have created a database and defined a process so that every project member participating in an event or responsible for the collection of a dataset will be able to insert selected actors and associate a structured description of them. These actors can then be monitored over time and across multiple platforms. This monitoring activity will provide us with the multi-platform data necessary to apply the multilayer network analysis methods.

2.4 Initial Analysis of the Network Data

As part of the activities planned in Tasks 2.3, 3.1 and 3.2 we have performed an initial analysis of the network data. While the analysis will be continuously updated and integrated until the end of the WPs, this initial analysis provides us significant insights and shows how quantitative and qualitative analysis can be integrated.

The initial data collection has been focused on Twitter data and included three types of hashtags. Event-specific, capturing tweets about e.g. a conference, Topic-specific, monitoring the discussions about specific concepts or activities (e.g. the development of proposals for IoT manifestos), and a general #iot hashtag that is intended to capture a large number of tweets without any specific focus apart from being related to the Internet of Things. The datasets corresponding to the first two types of tags can be then

explored using the software tools described in section 2.1.3.2, while the the #iot hashtag generated a massive dataset that requires a dedicated approach.

The initial analysis is based on the hashtag related to the set of IoT events monitored during our exploration of the research field (Task 2.1). Given a Twitter hashtag (#keyword) that represents a specific IoT event, all twitter activities (tweets, retweets, replies) containing that hashtag have been collected and stored at Uppsala University's server. The events covered by this report are the following:

Event Hashtag	Description
#BornHack	Bornhack 2017 - Danish maker/hacker event
#GIoTS2017	Geneva IoT Week
#iotconf17	Internet Of Things Conference, Malmo
#openiot	June 16th 2017 London MeetUp to revise 2012 definition and come up with a certification mark
#IoTWeek2017	Geneva IoT Week
#LTW	London Tech Week conference
#techfestival	Initiative exploring a new, progressive agenda on technology
#TechXLR8	IoT Conference – London
#Thingscon	ThingsCon Salon Copenhagen, as part of Copenhagen Tech Fest

A goal of the initial analysis was to investigate similarities and differences between IoT-related event and to use these event for an initial test of community detection methods. In order to do cross-event analysis over the IoT-related events, the Twitter communication networks of these events have been represented as a multiplex network . A multiplex is a network structure that models different modes of interactions among the same set of actors such that each mode of interaction is represented as a separate layer (or graph) in a multi-layer network structure.

The resulted multiplex is constituted of 9 layers (one layer per event), 9909 actors, 10547 nodes, and 11854 edges. In the context of Twitter based multiplex networks the actors represents the Twitter accounts, while the nodes represent the Twitter account active within a specific event. Within this perspective if the Twitter account @VIRT_EU

would have tweeted during #LTW and #openiot that activity would have resulted into two nodes but a single actor.

A first way to study differences and similarities between the various events is through the analysis of network density. Network Density is a network measure that describes the portion of actual connections among network nodes (the connections that exist) over

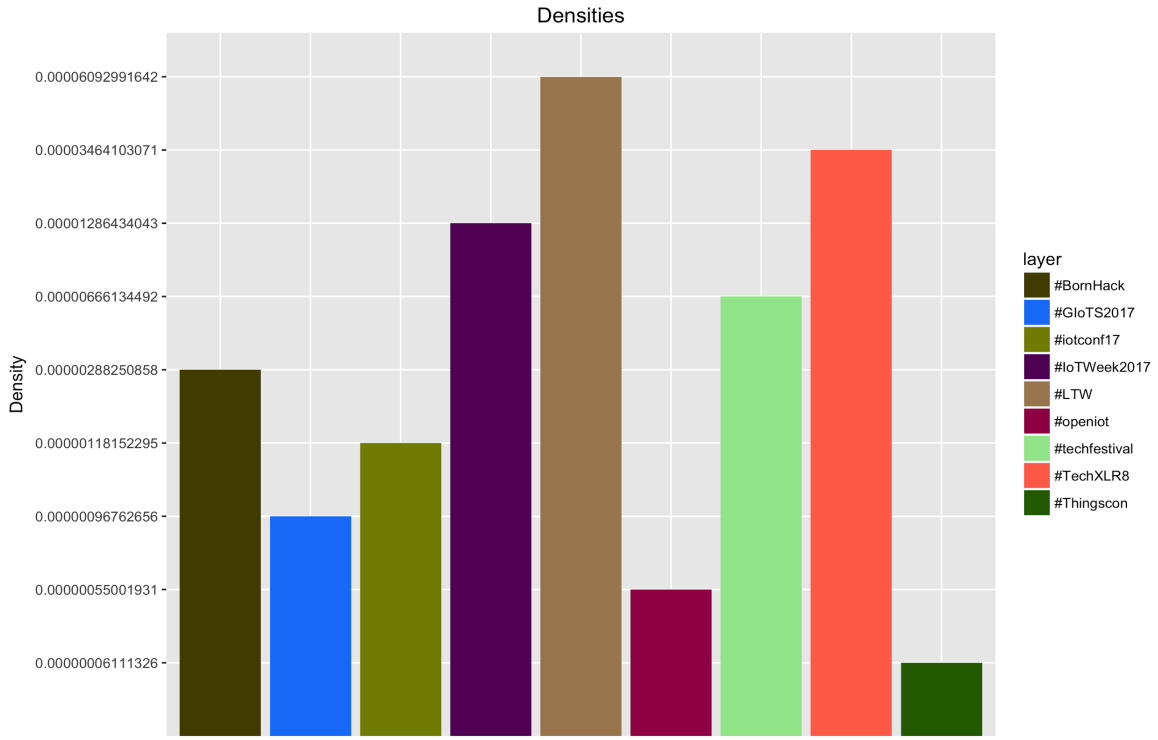

Figure 4: Density of the Twitter networks generated for the various IoT events analyzed.

the total amount of potential connections, and it is often used as a measurement of intensity of activity within the network. The following figure describes the densities of the studied events. It appears evident that events like London Tech Week conference, IoT Conference and London, Geneva IoT Week generated more densely connected networks than the other events. This means that during those event the interaction between the nodes were more frequent and the whole network was more active.

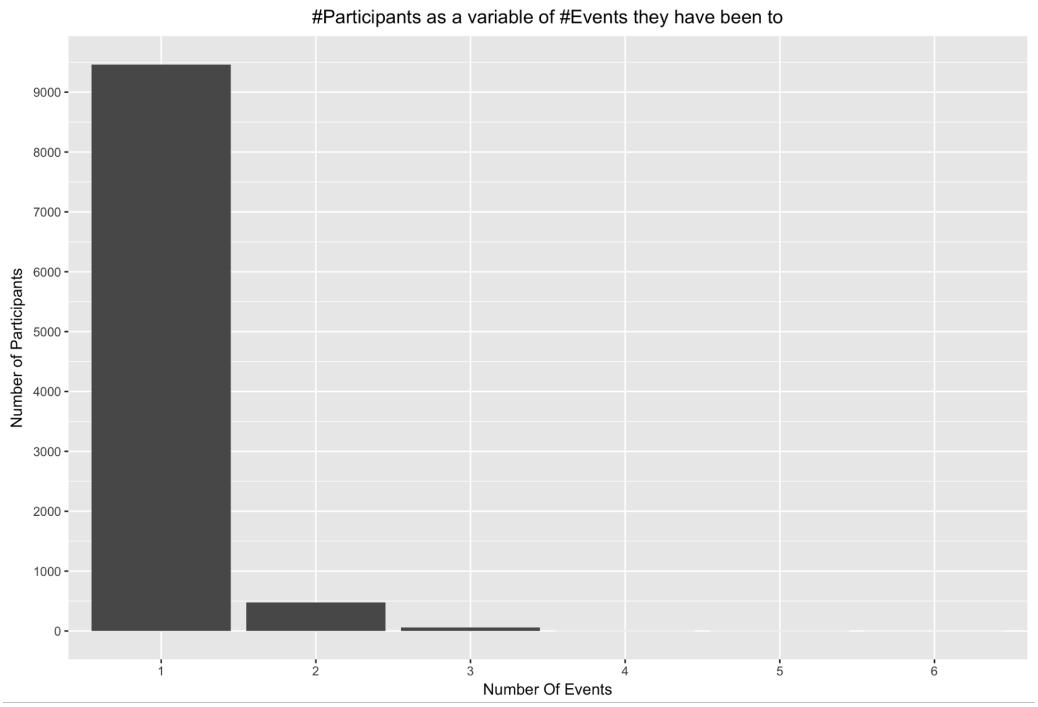
#Participants as a variable of #Events they have been to
Number of Participants
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
1
2
3
4
5
6
Number Of Events

Figure 5

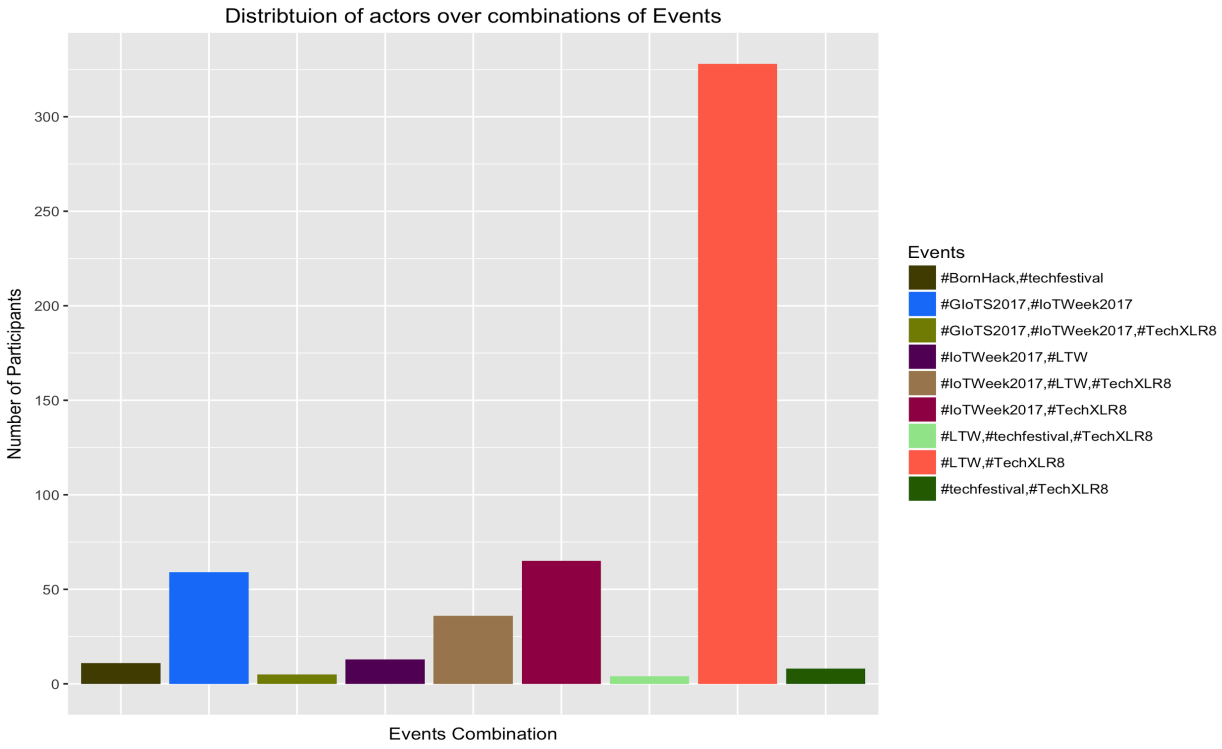

Figure 6

The overwhelming majority of the participants (actors) have been active only in one event (around 94%) while only (4%) has been active on two events (Figure 5). This data show two interesting dynamics. On the one side it shows how events that are located in geographically different spaces attract different non-overlapping communities. At the same time it shows the existence of a small number of users willing to “travel” to engage with different events.

It should be noted that even when we consider the nomadic actors (those who appear in more than one network) the majority of them have been active only in two events, with a very small number of users active in three of more events.

Figure 6 shows the distribution of participants over combinations of 2 or 3 events (after dropping all the results when the number of actors is less than 4). This support the interpretation that while the vast majority of users participate in the discussion about a single event there is a small group of users participating in multiple events. It should be noted that while all these events are located in Europe, they vary significantly on a geographical level.

As part of the activities planned in Task 2.3 we have defined three measures to evaluate similarity between various events. 1) Similarity based on actors: Similarity will

be measured on basis of the number of shared actors between two events. 2) Similarity based dyadic relations: the more the common ties (edges between the same two actors) among two events, the more these two events are similar. 3) Similarity based on actors' triangles: the more the common triangles (triads of edges among the same three actors) among two events, the more these two events will be considered similar.

The following tables show the highest 5 similar pairs of events for each similarity measure respectively. These three metrics of similarity help us observe how the similarity between various events is not just produced by users attending various events but to what extent those users were also interacting with the same people. The initial picture that emerges from the data is a picture where rather than observing actors that travel through different events we detect semi-stable groups of actors that maintain an ongoing conversation through different events.

Actor Similarity			**Dyadic relations Similarity**			**Triads Similarity**	
Pair	**Value**		**Pair**	**Value**		**Pair**	**Value**
#GIoTS2017, #IoTWeek2017	0.089		#GIoTS2017, #IoTWeek2017	0.068		#LTW, #TechXLR8	0.019
#LTW, #TechXLR8	0.044		#LTW, #TechXLR8	0.024		#GIoTS2017, #IoTWeek2017	0.015
#IoTWeek2017, #TechXLR8	0.034		#IoTWeek2017, #TechXLR8	0.005		----------	0
#iotconf17, #openiot	0.017		#techfestival, #BornHack	0.003		----------	0
#GIoTS2017, #iotconf17	0.017		#IoTWeek2017, #LTW	0.002		----------	0

Network analysis has proved over the years to be an effective method to identify central individuals within large and complex communities. While the concept of centrality is extremely complex and can be addressed in a number of ways, over the years a set of standard metrics to assess nodes' centrality in networks has emerged and consolidated. Among those measured, the degree centrality is undoubtedly one of the most commonly used. In social network analysis degree measures the connectivity of an actor with other actors. In_Degree: is the number of incoming edges to an actor. Out_Degree: is the number of outgoing edges from an actor. In our case the In_degree measures the number of times an actor was retweeted or replied to, while the Out_degree measures the number of times a participant retweeted or replied to other participants. The two metrics measures the relational activity performed by a specific users (replies and retweets done) or generated by a user's activities (replies and retweets received). Table

1 lists the highest 10 In_degrees, Out_degrees respectively with the corresponding participants' Twitter names.

In Degree			Out Degree	
Actor	Degree		Actor	Degree
LucioQuincioC	2330		TechXLR8	138
evankirstel	447		IoT_Forum	77
LDNTechWeek	416		LDNTechWeek	59
rparthiepan	351		Iotworldnews	48
akwyz	307		IoTimelab	40
TechXLR8	244		Emily_KNect365	38
BKaysac	163		5GWorldSeries	35
DrAhmad_Thuweni	159		Techfestivalcph	34
IoT_Forum	149		Cphftw	33
ericsson	125		ConferenceRepub	30

Table 1: In_Degree and Out_Degree. Top 10 users.

A closer look at the table offers several interesting insights about the activity that developed around the set of IoT-related events analysed. On the one side it is interesting to observe how - with few exceptions - the two lists are largely composed of different actors. This means that in the multilayer network we can find actors who seem to produce information and actors more focused on propagating that information. On the other side it is important to observe how while information producers (high Out_degree) are mainly official accounts of events and/or large organisations, information propagators are a more diverse group formed by organisational accounts as well as by "normal" users.

The last part of the preliminary analysis focused on the identification of communities within the data. The concept of community in the context of this project should be understood as a semi-stable cohesive group of users who seem to interact more frequently and/or on a regular based compared with the rest of the network. The specific nature of this initial dataset, with very few actors participating in more than one event, makes detecting communities an extremely challenging task. After careful consideration of several methods available for multilayer community detection we have opted for an approach based on Multilayer clique percolation[26]. While this approach is extremely restrictive in its definition of communities, it has a clear advantage of considering eligible for being assigned to a specific communities only the actors that are connected on at least two events. While this restrictive approach probably ignores a number of event specific communities it is able to focus on those communities that exist over various events showing a temporal and spatial continuity. This community detection activity, visualized in Figure7, shows the presence of 4 small communities that appears to aggregate around specific organisations (e.g. IoT_Forums), events (e.g. LDNTechWeek) or companies (e.g. ericsson).

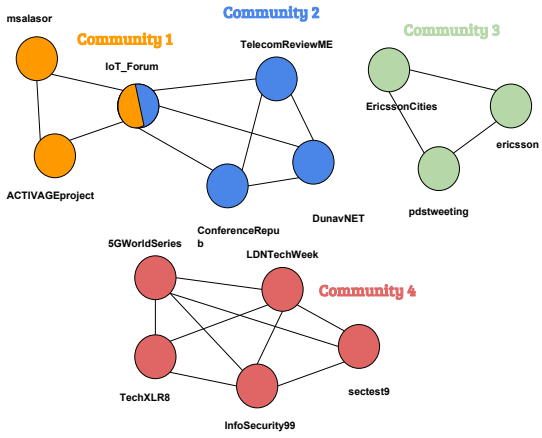

Figure 5: The communities identified from the multilayer networks of the IoT events

While the analysis of the quantitative data is still largely an ongoing activity, the results achieved so far appear extremely interesting. On the one side the comparative analysis of the various events has shown extremely low similarities between them pointing out the centrality of the local context into forging the events. Rather than being manifestations of a global community of IoT developers the events analyzed seem to be the materialisation of localised groups of interests. Nevertheless, the existence of a small group of actors who is travelling from one event to another has been detected, few central actors have been identified (both in terms of content producers as well as in terms of content sharers) and the kernel of a potentially larger community structure has been observed. These insights were integrated with the ethnographic part of the domain exploration described in the following section.

[26] Afsarmanesh, N., & Magnani, M. (2016). Finding overlapping communities in multiplex networks. *arXiv preprint arXiv:1602.03746*.

3.0 Domain Exploration and Identification of Informants in European Centres of IoT Innovation

In this section we outline the results of our mapping of key ethical perspectives as they appeared across the law, sociology, communication studies and design literature, our identification and description of the key actors seeking to define the IoT and/or surface its ethical dimensions, and a summary of ethical issues identified in preliminary fieldwork, including interviews, observation and analysis of 'IoT manifestos' that specifically highlight alternative positions to ethical issues that designers and advocates themselves identify. Finally, we identify methods for pursuing the occasion of the ethical IoT through several field sites identified in our domain mapping (Tasks 2.1; 2.2).

3.1 Ethnographic Domain Mapping

Through fieldwork in London, Geneva, Lyon, Torino, Copenhagen, Bled, Malmö, Berlin, and Barcelona our project team were able to map the most commonly expressed ethical values and reflect upon how these values were discussed and instantiated (Task 2.3). Ethnographic methods such as observations, extended field notes, interviews, and document and policy analyses have been used thus far to make sense of emerging data practices, responsible research and innovation (RRI), and data ethics at the point of design in relation to the Internet of Things. Alongside these exchanges, formally planned, semi-structured interviews were conducted with a range of IoT community participants. Observational research included a mix of both non-participatory observations and participation in certain events such as policy development working groups and presenting papers at conferences.

Initial locations were chosen based on indications of IoT innovation and investment in particular locations, especially London and Amsterdam, due to clustered research, civic innovation, and SME industrial contexts (Tasks 2.1; 2.2). Across these contexts, researchers observed sets of values and interests, continuously following traces and cues from IoT developers encountered along the way. Besides noticing the values underlying IoT development an initial attention has been directed towards what ethics means to different IoT developers articulated through informal conversations, presentations or discussions during these engagements. We still have not entered sites where IoT technologies are created and followed the daily practices of developers, but based on initial research it is clear that ethics in IoT is not easy for developers to define or localise (Task 3.3).

Entering the field of European IoT development we have initially been faced with a huge space from a qualitative point of departure. During the first phase of the project (focused on an ethnographic domain mapping) we worked with a broad fieldwork scope (Tasks 2.1; 2.2) that in the next phase of the project will be narrowed down to geographic locations and selected development sites for more in depth ethnographic inquiries (Task 3.3). During the first part of the project we attended the following events across Europe

which embrace both large IoT conferences and smaller meetups to draw the contours of the European IoT scape (Task 2.2). Throughout the deliverable we intend to go deeper into analytical insights from these events playing a crucial role for our choices of field sites for more in depth ethnographic inquiry (Tasks 2.6; 3.3).

Geographic location	Event	Date
Barcelona, Spain	Startupbootcamp	January 4, 2017
	4 Years From Now (4YFN)	February 27-March 2, 2017
	Mobile World Congress (MWC)	March 2, 2017
London, UK	Connected Seeds and Sensors	February 1, 2017
	Advisory Panel: The Impact on the Internet of Things on Managing Work (Loughborough University research project)	February 22, 2017
	Smart IoT London Conference	March 15-16, 2017
	MEETUP: IoT London	March 21, 2017 - ongoing
	ZAIZI 'Data Driven Government Roadshow'	March 23, 2017
	WiTT (Women in Telecoms and Tech) meeting: Insights from Mobile World Congress 2017	April 20, 2017
	Avren's World: IoT Networks Conference	May 23-24, 2017
	TechXLR8 Conference	June 12-15, 2017
	Expert workshop on citizen/consumer engagement with policy-making for Internet of Things	June 13, 2017
	IoT Trustmark: Day 1	June 16, 2017
	IoT Trustmark: Day 2	September 11, 2017
	Organised IoT Trustmark event	September 24, 2017
	FixFest	October 6, 2017
	The Ethics of Coding and the Human Algorithmic Condition: The Algorithmic Condition Workshop	October 10, 2017
	NetGain Partnership Event on Algorithmic Accountability	October 25, 2017

Berlin, Germany	Open IoT Studio, Mozilla	March 23-24, 2017
	ThingsCon Salon	March 23, 2017
Lyon, France	The IoT Showroom (SIDO)	April 5-6, 2017
Torino, Italy	Mini Maker Faire	May 27-28, 2017
Copenhagen, Denmark	The Internet of Green Things Festival	April 10, 2017
	The Things Network Hackathon	June 1, 2017
	ThingsCon Salon, TechFest	September 6, 2017
	Dowse Workshop	November 2, 2017
Geneva, Switzerland	IoT Week	June 4-7, 2017
Bled, Slovenia	Living Bits and Things	June 19-20, 2017
Malmö, Sweden	IoTConf.se	May 23-24, 2017

Within our fieldwork, ethics did not initially emerge in a straightforward manner. To map the domain, we focused both on 'dominant' perspectives related to ethics and IoT and on 'alternative' perspectives that took critical or oppositional views to these dominant positions[27]. Using a set of participatory, ethnographic and interview methods, we observed how values as enactments of ethical practice were discussed at Europe's high profile IoT conferences and working group presentations, on company websites, IoT declarations, and in promotional literature. The interviews, observations and participation in events were also supplemented by an analysis of 'IoT manifestos' that ostensibly occupied alternative positions in relation to the dominant values (Task 2.1; 2.2; 2.6). The sections below describe how values are presented and negotiated across dominant and alternative positions.

3.2 Discussions of Ethics within Communities of Practice

Our research has shown that moral reasoning and ethical conduct are rarely topics for discussion online or offline in some communities of IoT developers and innovators. Few people ask: how do we figure this out? As one developer emphasised: "Ethics is like this big elephant in the room whenever IoT is discussed." Informed moral reasoning includes recognising that there are ethical implications embedded in both assumptions and decisions about product or service design. For example, with vast amounts of categorisation occurring as a result of the data gathered via IoT devices, who is asking how these categories are made and what the benefits or consequences of the categorisation will be for those defined in this way.

[27] Mansell, R. (2012). *Imagining the Internet.* Oxford: Oxford University Press.

Connected devices and services are increasingly designed as part of mundane infrastructure, effectively rendering their internal processes of data-gathering and external processes of data-movement or data-storage invisible. However, developers have the opportunity to design these crucial processes of data use in alternative, or more fitting, ways if they are aware of the potential trade-offs they are making while creating the connected devices/services that are part of our mundane infrastructure. To offer a practical example, while the use of a cheaper component would benefit the bottom line, might this also be considered a security trade-off? And while the decision to design a device interface might require data being routed via cloud as an easy solution, what does this requirement mean for end-users wanting to protect the fragile hold on privacy they might have left?

Relatedly, findings derived from initial domain exploration (Task 2.2) show that certain individuals and groups are unable to explicitly articulate values that potentially drive their actions. While this does not suggest an absence of values, it might suggest that there is a tacit value system that sits beneath a vocabulary to identify these concepts as such. For instance, there are implicit values in manifestos and promotional materials that upon a close reading can be unearthed as specific values relating to social justice. There are also explicit values that companies insert into their social responsibility schemes. Some of these motivations might point toward a desire to situate the company in particular movements (e.g. the Circular Economy movement with their explicit statements on social and environmental justice).

Other motivations revolve around a company branding themselves in a particular way to generate profit or obtain grants. How identification of values occurs, then, sits on a scale of tacit to explicit with evidence strongly suggesting that a vocabulary is missing to identify values other than those already established as the norm. In order to begin making sense of the complex ethical landscape of IoT design and development, the preliminary ethnographic research presented in this section is focused on the tacit and explicit values emerging in various IoT contexts across the EU.

When openly invited to think and talk about ethics in IoT, many developers especially at some of the bigger IoT conferences we have participated in (SIDO, 4YFN, MWC), point to *privacy, security* and *data*. However, these three central themes do not necessarily appear as a full package. Some developers might point to privacy, others to security or data. As an Italian developer of a smart home assistant asked when posed an open question about ethics in the development of this particular IoT technology at the Mini Maker Faire in Torino: ‘Do you mean privacy *or* security?’. This example suggests that, for him, there are two major topics related to ethics in IoT development processes, and that it can be one *or* the other. He posed the question because privacy and security have very different practical implications in the development process. What we are finding is that the creation and enactment of virtues is relational, varying in degree and kind across diverse contexts, and often subject to dominant cultural and economic frameworks. Here we present some of the most commonly encountered ways of talking about ethical issues: in relation to *privacy* and *trust, security, data management,*

responsibility, and *openness* and *interoperability.* We also discuss how use of the IoT in personalised sensing is understood in relation to *wellness* and *care.*

3.2.1 Privacy

Privacy was a primary value that appeared in all settings. The dominant notion of privacy, however, seemed to be more related to informational privacy/data privacy than any other form of privacy, such as concepts pertaining to dignity or integrity of body (e.g., questions around whether or not nanotech connected to IoT ought to be inserted into the body for health-related data are not yet extending to privacy as freedom from biological monitoring systems). Notions of privacy were also embedded with assumptions based on reasonableness which remains a concept difficult to pin down with any real consistency. In other words, what one company might consider reasonable consumer data collection might not be thought of in the same way by another company.

Many people we spoke with seemed to be thinking about these concepts from a legal framework in that they do not want to be sanctioned for doing things the 'wrong way'. Some people identified a gap between their identity as individuals and the values or principles that might be held by an organisation, identifying privacy and data protection as ethical ideals. One of these individuals in particular explicitly pointed out that she is not simply part of industry, she is also the public, so she was speaking about privacy and data protection as processes that are necessary and important for the social good.

These frameworks conflict and overlap: people at the large industry IoT conferences we have participated in (SIDO, 4YFN, MWC) may point to *privacy, security* and *data* when asked about ethics, but these themes may not necessarily appear as a full package as mentioned previously. Some people might point to privacy, others to security or data. Others are thinking about privacy and data protection as tools that can help them manage their company image or brand. Privacy, then, is being used as a marketing tactic. In this capacity, privacy and data protection are situated as economic values in line with a perspective that holds market competition to be the greatest virtue.

In addition, privacy here does not seem to take seriously freedom from behavioural advertising as an incursion into privacy of intellectual life, especially in the case of children. Although children are better protected with the incoming GDPR regulations, these requirements do not seem to be relevant to some IoT developers as their value systems appear to be focused on freeing businesses to be innovative. In their opinion, as advertising is central to a successful business model, advertising should not be constrained by an ethical principle related to intellectual privacy.

The value of privacy and IoT is well articulated by a privacy expert interviewed in Geneva. He claimed that companies are now more willing to comply with privacy rules to establish an image of being part of a "trusted IoT ecosystem". In this capacity, there has been a shift in the IoT discourse from the centrality of interoperability to include a realisation that there is something more: privacy is now increasingly being perceived as a primary value, and as an object that can be leveraged for marketing purposes:

“Privacy has become an asset to build reputation.” While some companies have integrated privacy as part of corporate social responsibility, other companies are engaged with privacy as an economic imperative.

3.2.2 Trust

Similar to the discussions around privacy, trust - a related concept - is also framed in relation to public perception. It does not present as a value that is being upheld for what some might consider classically virtuous reasons; rather, it is being promoted for profit generating and marketing purposes. Companies are seeking to acquire the public’s trust in technology, to overcome socially pressing issues such as food production, or energy management, for example. In order to do this, privacy is being used as a means for the acquisition of public faith and trust. A Bosch representative put it this way: “Getting trust in a connected world is truly the key”.

3.2.3 Data Protection

Most discussions about data protection that we heard in our domain mapping centre around ideas of unfair use of data which predominantly relates to malicious acts such as hacking which could result in ‘unfair’ use of data in terms of fraudulent activity, for example. The most common themes emerging in the discussion of data protection relate to *data ownership.* Here, questions often arise around whether or not the consumer owns their data, whether ownership is shared with the company, which might also mean, in some circumstances, that it is traded/sold to other third parties. Also related is the fact that regulations around data collected (selling and sharing to third parties) seem to be skirted by companies extracting data and creating reports, then labelling these reports as “knowledge’. As such, ownership and sharing of consumer information is justified as ownership and sharing “knowledge” instead of sharing and selling “data” which bypasses a whole system of consumer data protections.

There has not been explicit and sustained discussion of the relationship between discrimination and data use. When pressed, individuals and groups have stated that while they are aware such things exist, in terms of policing for instance, most do not think about discriminatory use of data in relation to their own work with IoT. As an extreme example, one start-up was emphatic about the impossibility of companies using the data generated from IoT apps in discriminatory ways. The start-up in question had created an app that was being sold to large companies such as Starbucks to “contextualise” customer habits. The app was able to capture a customer’s likes and it also had the capacity to generate information derived from customers’ geo-spatial activities. Along with tracking daily routines and coffee preferences, with a built-in GPS, gyroscope and accelerometer,

Starbucks could use the app to determine whether or not the user was a “safe”, “dangerous”, “anticipative”, “distracted”, or “illegal” driver. Starbucks could also tell if the user was a “green commuter”, “healthy worker”, or “shopaholic”. The vast amounts of data that this app was able to capture seemed to have quite serious repercussions for

consumers should the data be connected across companies, especially in the case of insurance companies. The co-founder of the start-up did not seem to be concerned about the potential for insurance companies, for example, to use the app to make discriminatory decisions based on geo-spatial or demographic data.

3.2.4 Security & Safety

There is a general consensus that security considerations should not be optional add-ons, but rather, should be considered at the point of design and throughout the lifecycle of IoT applications. However, people we spoke with identified that security, which is related to data protection for both consumers and corporations, is not something that all companies can afford to do, especially not start-ups with limited financial resources. The argument from start-ups tended to be that embedding security into a device is costly, so they were willing to take the risk of not doing 'security by design'. Larger companies, however, have the financial means to take security by design seriously which potentially gives them an advantage over the smaller companies when it comes to obtaining public trust. Relatedly, *Security hygiene* has been a recurrent term when addressing how to protect the IoT from malicious attacks.

Safety is also often linked to security. The idea of safety has been debated at length during various conferences, and is a value that is more predominant in certain sectors over others. For instance, safety is paramount in IoT sectors such as health, automotive, and industrial IoT. It is also prevalent in the discussion around commercial IoT drones with regards to aviation rules and regulations. On the other hand, security and safety have been used as values that justify increased monitoring of populations, sometimes also linked to ideas of efficiency which characterize discussions of the Smart City and wearable devices, along with the notion of *wellbeing*.

3.2.5 Wellness & Care

A range of IoT goods and services are marketed as serving consumer health and wellness. As such, well-being is certainly emerging as a primary value in the IoT environment. These ideas are most evident in the case of sleep, fitness, development, and mental health monitors. For example, one start-up has developed "a novel way" to monitor and track a child's early development by combining state-of-the-art baby monitors with a child development tracker service that could be accessed remotely. However, the company, like many others, had not completely mapped out plans to address issues of data security and issues of consent, especially in the case of the GDPR requirements.

Another start-up had developed an app that could identify and monitor employees' mood from their voices. By analysing correlations between weather information and moods, the app had the capacity to forecast diurnal and week-to-week variations of a person's mood. Through an admin dashboard, employers could check individual and team moods, which was justified as helpful for improving employees' motivation and well-being. While the company founder claimed that it is in the best interests of the

worker if the company knows how employees are feeling, there are personal privacy issues that emerge when external parties have the right to monitor employee mood states on a continuous basis.

3.2.6 Responsibility & Design

Responsibility and liability have tended to emerge together. Individuals and groups have spoken about responsibility' in general a lot (both private and public sector); however, most start-ups have not explicitly spoken about the idea of 'responsible innovation', although the terminology exists in the EU documents/reports that explore IoT technologies. Ethics by design was discussed at the Open IoT Trust Mark event in London, as were ideas around responsible innovation in the context of respect for human values and human dignity. Responsible innovation was also taken up by a handful of developers at the same event, but in the context of environmental stewardship.

Some IoT producers outsource software development, which means that responsibility for product failures or ensuing harms have become difficult to pinpoint. While these companies seemed to take their responsibility to consumers seriously, the software developers contracted by IoT manufacturers generally claimed that if the product were to cause harm somehow, liability rested on the manufacturer of the hardware itself and not with the software development. In this sense, responsibility was being passed on by software to hardware. The issue of responsibility was also a value that emerged from consumer rights groups concerned about the recourse an individual could take if an IoT company went out of business and the end-user needed regular software updates.

3.3 Alternative Positions on Ethics: IoT Manifestos

The expression and discussion of debates in relation to the values associated with IoT technologies across our domain mapping fieldwork show how many ethical claims are positioned in relation to marketing claims. Findings also suggest that law, regulation, and manufacturing contexts nuanced how people talked about values.

An example of both online data collection and initial domain exploration (Tasks 2.1; 2.2), a second empirical exercise conducted showed that over the last several years there has been a proliferation of public statements, manifestos, and calls from advocates, designers, and developers for negotiating alternative or oppositional positions for the IoT, often specifically referring to ethics (although also to values in general). Emerging from a sense of uncertainty, the manifestos create publics for debate, demand attention and call for change.

Manifestos are 'a battlefield' or 'a loud invitation to think in new ways'[28] and the proliferation of manifestos among designers and developers of IoT and other connective technologies is clearly indicative of a need for change. It is as if the framework of

[28] Parent, M. (2001). The Poetics of the Manifesto. Newness and Nowness. In *Manifesto. A Century of Isms.* University of Nebraska Press, x–xxxi.

technological modernism[29] focused on progress, rational planning, and improving the world through technology is frustrating those charged with changing the world in its inadequacy to address the looming crises. Writing a manifesto is to participate in a history of struggle against dominant forces linking one's voice to the countless voices of previous revolutionary conflicts[30] and it is important to ask: what (potential) revolution is called for and underway?

In an effort to chart the particular challenges and to review the stated concerns, we analysed the content of 28 documents that we have classified as calls for action toward responsible technology development in Europe. All these documents were published between 2011-2017 and arise from European contexts (for a full list of manifestos see Appendix I). We note that while the manifestos in question provide potential roadmaps for a better future, they also express a deep concern and even fear of the state of the world and the role of technology in it. When each of the 28 manifestos stand-alone a great deal of *certainty* and assertiveness is expressed in the genre– they call clearly for change. However, reading them alongside each other shows that commonly articulated *uncertainties* underlie and trigger the manifestos.

Indeed, these documents draw our attention to a general feeling of an impending apocalypse – exacerbated by IoT – a negative picture that becomes the grounds from which to express change for a better future. In our analysis, we identified concerns that manifesto authors share including worries about *ubiquity* and *invisibility* of devices. In addition, we noticed how the same ideal values that emerge in their dominant form through our interviews and observations are contested: *Openness* and *Sustainability* are interrogated, and *privacy* and *control* placed in relation to these values, rather than as marketing fodder. These threads merge under *Responsibility* running through all manifestos where, having identified key areas to address, authors begin to nominate normative pathways for specific actors to make changes.

3.3.1 Ubiquity & Invisibility

The manifestos move past the dominant frameworks of ethics as a marketing ploy. Drawing an apocalyptic picture of the present state of IoT characterised by surveillance, bots with agentive capacities and leaking data. In fact, some authors align the development of IoT with far-right nationalism, ongoing wars and climate change strongly underscoring the scale of the problems they believe we are facing.

Estimations and expectations of IoT development are reflected upon in many manifestos, which mention the rapid growth of IoT but also concerns about the worrisome or malicious aspects of IoT. The pace and intensity are marked as worrisome: "New technologies are being developed at a pace which even the most native of digital natives find it hard to follow. The future is not just digital, it's super-digital, and we cannot even begin to imagine what our lives will be like in 15 or 20 years, for better or worse" (RIOT, see Appendix I).

[29] Sengers, P. (2007). The Ideology of Modernism in HCI. *Position Paper*.
[30] Lyon, J. (1999). *Manifestos: Provocations of the Modern*. Cornell University Press.

Authors also worry about the ubiquity of IoT devices, returning to concerns highlighted over the past twenty years[31] including visions of computers 'disappearing into the background'[32]. 'Ubicomp' is implicated in the broken promises that often drive the production of manifestos[33]. Manifestos raise a critique of the dominant ideal of progress characterizing modernity and the manifestos we have analysed reflect on the envisioned ideals for progress in the technological development that IoT is part of. Manifesto authors seem worried about what ubiquity means now that it is here and connect it to manipulation, surveillance, privacy and security concerns and more.

Ubiquity is made more problematic because of invisibility. Invisibility is directly contested as a central value feeding into the development and life of IoT technologies. Invisibility here characterises the complexity of technologies and the processes behind their creation and workings that are difficult to see through. A number of manifestos call for transparency relating to how technologies and algorithms work, what data is collected and how technologies impact our world, presenting alternative views on the values of transparency, openness and sustainability – which the manifestos present as core values. They re-present values such as privacy, security and responsibility in relation to these core values.

3.3.2 Transparency

Alternative frameworks focus on transparency as a value that connects ethical perspectives and consumer choice is an important aspect of thinking about IoT, but how is a consumer to make an informed decision with the proliferation of IoT devices? IoT technologies enter critical parts of life and gather extensive amounts of data and insights about their users, where bad handling of data can have crucial consequences. Many documents in our analysis espouse the belief that transparency is both essential and possible and suggest two main approaches to be adopted by creators of or contributors of IoT devices. One is to design IoT services that are trustworthy and help users understand how they work. Another is to create something that can help consumers make more informed decisions. For example, the grassroots development of an "IoT trustmark" seeks to involve European IoT community members in discussing and defining which aspects of IoT development might be made transparent. This project is itself an alternative argument in support of a vision of Open IoT development, and has emerged as a key site for ongoing research.

3.3.3. Openness

The ideal of openness carried an overwhelmingly positive connotation across our corpus of documents. It was connected with equality (access for all) and community

[31] Kaye, J. and M. Wright Steenson. (2017). Theme Issue on Histories of Ubicomp. *Personal and Ubiquitous Computing,* 21 (3), 553–555.
[32] Weiser, M. (1999). The computer for the 21st century. *Sci Am,* 265 (3), 94–104.
[33] Lyon, J. (1999). *Manifestos: Provocations of the Modern*. Cornell University Press.

building. It was seen as central to challenging dominant power structures and to democratizing control. While manifesto documents argued forcefully for open hardware, open software and open standards, none promoted the idea of open data perhaps in an effort to acknowledge the issues of privacy. Yet the paradox of openness is that it is not possible to include everyone. Thus the rhetoric of openness, while positive, does not allow a discussion of exclusion even as its structures exclude those who disagree[34]. Light at al. argue that a "robust and inclusive community is always desirable"[35] yet communities are always bounded, articulating those who do and do not belong. Thus openness, for manifesto authors, has a double-sided nature that also suggests the exclusivity of an 'open' framework that only allows some to permit, for example people with better technical knowledge.

Elsewhere in our fieldwork, the IoT Trust Mark working group evoked openness in their efforts to define an open IoT mark carrying ethical principles for IoT design. The project assumes that such products have digital information or 'data' as a driving mechanism or a by-product and are mostly commercial in nature, which means an identifiable company or group of people are responsible for its creation, manufacturing, distribution. As such, based on the value of openness, the project seeks to offer industry an instrument to support and encourage more ethical data, product, service and manufacturing practices; provide a way for industry to demonstrate a commitment to consumer rights in IoT products; help improve consumer literacy in understanding the constraints, opportunities and consequences of their use of IoT products, enable consumers to make better decisions about how they use such products; and using best practices in software, hardware and product design, help consumers have access to a choice of higher quality, trustworthy connected products which protect their interests as consumers and people.

3.3.4 Sustainability

At least 13 manifestos express concerns about sustainability in IoT returning us to the question of progress both in the manifestos and in HCI. Technology design is implicated in an impulse to create change and often seeks to create social change through technological development[36]. Much of this research turned problems of environmental action into questions of personal moral choice, often focusing on behavior change as a route to altering individual consumption patterns[37]. An alternative path has been to

[34] Nafus, D. (2012). 'Patches don't have gender': What is not open in open source software. *New Media & Society, 14*(4), 669–683.
[35] Light, A., Powell, A., & Shklovski, I. (2017). Design for Existential Crisis. Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, ACM, 722–734.
[36] Håkansson, M. and Phoebe Sengers. (2014). No Easy Compromise: Sustainability and the Dilemmas and Dynamics of Change. *Proceedings of the 2014 Conference on Designing Interactive Systems*, ACM, 1025–1034.
[37] Dourish, P. (2010). HCI and Environmental Sustainability: The Politics of Design and the Design of Politics. *DIS '10. Proceedings of the 8th ACM Conference on Designing Interactive Systems. August 16-20, Aarhus Denmark*, 1–10.

focus on 'ecologies of practices' *within* design and HCI[38]. Although sustainability is an important ideal, it is the latter approach that is more apparent. Just a few documents imagine how IoT could be used to change, augment or improve individual behavior. We identify three important conceptions of sustainability in the documents. One deals with realigning lifetimes of the physical and the digital, the second with obsolescence and the third with locality.

IoT products are part service and part infrastructure, but the lifecycles of physical objects are longer and do not match the temporary nature of contemporary software development[39]. Several documents call for a re-alignment of digital and physical lifespans, addressing the problem of firmware and software updating that can often render unusable perfectly functional hardware components.

The practice of constant update has extended to hardware especially in cases such as mobile phones but many documents warn that such practices are only harmful. Current business tactics tend to devalue the ability to repair, recycle and repurpose code as well as materials and design tactics to be employed. The mismatch between lifespans of hardware and software has led toward a business tactic of creating demand for new devices with intentional obsolescence as pointed to in some manifestos. Overcoming obsolescence then requires that hardware should be designed for reuse, repair or recycling.

In a variety of ways, the local in many manifestos relates to context and the processes of which IoT technologies are inevitably a part. As promoted in sustainable thinking no action or creation stands alone or outside an ecosystem as influence neutral and this also counts for IoT development. IoT technologies cannot be separated from the contexts they operate within.

3.3.5 Control & Privacy

In addition, running through all the themes in the manifestos addressed above, questions of *control* and *privacy* are central even when not explicitly appearing in a conceptual shape. Or put in another way: searching for 'control' and 'privacy' directly in the manifestos only partially leads one to the role these phenomena play in the texts. In the manifestos dealing with ubiquity, invisibility, transparency and sustainability questions of privacy and control present themselves more implicitly while they are explicit and important topics in the manifestos promoting openness as a central value in IoT.

Questions of privacy and control are mobilised in reflections about what a ubiquitous and invisible infrastructure entails, in one manifesto with reference to Baudrillard's

[38] Pierce, J. Yolande Strengers, Phoebe Sengers, and Susanne Bødker. (2013). Introduction to the Special Issue on Practice-oriented Approaches to Sustainable HCI. *ACM Trans. Comput.-Hum. Interact*, *20* (4), 20:1–20:8.
[39] Nafus, D. (2012). 'Patches don't have gender': What is not open in open source software. *New Media & Society, 14* (4), 669–683.

thoughts about how "*we are way beyond the Panopticon, of visibility as a source of power and control*". Now expressions of power and control are about erasing traces of their operation. Living in a world where these technologies are ever present yet invisible to most people highlights issues of privacy, data collection, control and processing. Curiously, one of the ways of addressing the problems of invisibility appears to be a call for openness.

Though there is an apparent tension between values of openness, control, and privacy manifestos promoting openness explicitly deal with questions of privacy and control. Openness in these documents is positioned as a way to combat surveillance and to democratise control. Some are advocating that users must be able to control their digital lives and connected products and services while celebrating open innovation and sharing. Dowse also promotes openness and yet it is a software designed to give the user control and deal with privacy concerns: "*Dowse keeps your private network private*" and an On-OFF button that is often missing in IoT allowing people to disconnect.

In the manifestos flagging concerns in regards to sustainable matters, issues about control and privacy are raised on a planetary scale and reflect challenges we are facing in the Anthropocene[40]. Uribe opens the notion of control beyond the human as IoT technologies might harm other forms as life. How does an animal living with IoT claim control? How do environments claim privacy and control when actions in the development of IoT and beyond clearly impact and intervene in natural processes all over the world? The questions tackle global warming and the role IoT technologies play in this scenario. Many implicitly raise critique of current technological progress willfully ignoring questions of longevity and obsolescence. An infinite desire for expansion and excursion of control also manifested in technological development is now challenging the future, ironically enough, potentially beyond (human) control.

3.3.6 Responsibility

Connecting to widespread anxiety about technological futures, Light et al. challenge designers to take responsibility for our collective futures, acknowledging their responsibility as its architects[41]. Responsibility is a crucial area of reflection for the document creators. Responsibility here is raised in relation to specific concerns. We have localised three thematic clusters dealing with responsibility in the manifestos: *Understanding, Debate & Dialogue* and *Togetherness*.

3.3.6.1 Understanding

The 'understandability' of IoT devices, of their design, of their data management and of the potential consequences of their use is strongly associated with calls for greater responsibility. Across the manifestos the majority of statements were addressed to designers and creators of devices. Few pointed to the need for citizens to be educated,

[40] Light, A., Powell, A., & Shklovski, I. (2017). Design for Existential Crisis. Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, ACM, 722–734.
[41] ibid

such that they might understand, choosing instead to orient on the need for designers to make their products, processes or agreements understandable. As a responsibility, '*making understandable*' takes a range of forms, but the majority focus on clarity of language and explicitness of processes involved in using an IoT device.

3.3.6.2 Debate & Dialogue

Shifting the emphasis from the relationship between designers and users we turn toward the meaning of design. Under this heading, we find a number of strategies oriented explicitly at designers and their activities, from calls for debate to attempts to develop common agreements about norms. While some manifestos show that some individuals, companies, and firms have a clear idea of what responsibility for helping people might look like, others are more interested in sparking dialogue about what responsibility itself means. If responsible design must be more than 'adding technology', then how could it be done? Many authors position their community as responsible for dialogue, arguing that its members have a valuable contribution to make to ensure a future where IoT works for everyone, demanding actionable guidelines for starting conversations.

3.3.6.3 Togetherness

In addition to promoting conversation, debate and dialogue, manifestos invite readers to participate, to commit, to take action and to take responsibility. This move aims to create a bond between the individual signatories as a community, a move toward concerted effort and – potentially – mutual accountability for responsible behaviour. Yet there is a distinction between addressing a 'we' of writers and readers, and the 'everyone' of stakeholder engagement. Attention to the acts of inclusion and distribution within calls to responsibility and make us attentive to the politics and practicalities of *responsibilisation*. While responsibility is something most authors want, there is little agreement on the nature of that responsibility, the subjects or groups to take it on, or the ends it has in sight.

Paying attention to where and in whom authors locate responsibility complicates the picture of how change can be effected. IoT is framed as a complex system, wherein it might be difficult for single actors to identify the effect of their actions. The proposal – to use IoT to integrate feedback, or 'consequences' - is about the responsibilisation of actors using IoT as a conduit. In this synthesis, design takes responsibility to make others take responsibility – the latter in the broadest sense: responsibility for consumer choices such as the environmental consequences of 'buying a banana in winter-grey Berlin'.

In the shift from what is possible to what is desirable, the manifestoes draw upon responsibility as a resource to think with. However, the ways they do so, and how responsibilities get allocated, are markedly different. Responsibility for ensuring understandability is something design communities are exhorted to take upon themselves.

The very nature of design responsibility – its potential and its breadth – comes under discussion. In drawing out these distinctions, we have pointed to how readers of manifestoes are invited to participate in a project of change, sometimes with specific ends in mind, sometimes with specific 'responsible' products in mind, and sometimes simply towards further and deeper dialogue. While responsibility is something most authors want, there is little agreement on the nature of that responsibility, the subjects or groups to take it on, or the ends it has in sight.

3.4 Alternative Ethical Frameworks

Across the manifestos, as authors seek to connect human flourishing to design potentials and decisions, they illustrate that the audiences generated by manifestos occur around an identification with virtue and its oppression by hegemonic forces[42]. Yet designers and developers are lauded as having a particular position, and a particular responsibility at this 'crossroads' as perhaps best prepared to envision the 'right' future.

What *all* manifestos analyzed share are efforts to relate to an intangible and rapidly developing world they are themselves part of creating through technological development. This relational effort is an expression of IoT as a matter of care and suggests the importance of considering practice-based ethics. The next section investigates how this can unfold through the use of virtue ethics perspectives.

3.5 Applying Virtue Ethics in the Study of the IoT

It is evident that ethics has come to have many meanings. In general terms, however, ethics concerns the frameworks and principles that define our ability to lead a good life and to conceptualise our rights and responsibilities. In many fields of ethics, these frameworks and principles are either considered in terms of outcome, as in consequential ethics, or in terms of universal rules, as in deontological ethics[43]. In the fields of technology and information, rules and frameworks – deriving from a consequentialist approach – have been the most common mechanisms of assessing and governing ethics. Yet it is increasingly evident that when ethical frameworks are externally imposed on communities of practice they can fail through ignorance of existing enacted ethical practices and a community's contextual constraints[44]. While some research participants have claimed that the uptake of new technologies and values will always be governed by the market, others believe that there are diverse forces at work in terms of resistance or acceptance of new technologies and the values and principles that accompany such technologies. These forces range from non-market institutions to grassroots groups who are seeking to protect the best interests of the public, for example.

[42] Lyon, J. (1999). *Manifestos: Provocations of the Modern*. Cornell University Press.
[43] Berdichevsky, D, & Neuenschwander, E. (1999). Toward an ethics of persuasive technology. *Communications of the ACM 42.5*, 51-58.
[44] Feenberg, A. (1998). *Questioning Technology*. Oxon, OC: Routledge.

Virtue ethics can be traced back to the philosophical writings of Plato, Aristotle, Socrates, and the Stoics. A central tenet of virtue ethics is that all moral agents hold a final good towards which immediate aims are directed, and against which these aims can be evaluated. All questions attached to right action are assessed against this final good which is generally identified as *eudaimonia*[45]. Following their ancient roots, contemporary iterations uphold as fundamental the question: What it is that will enable the agent to lead a life characterised by *eudaimonia*?[46].

It is commonly agreed that *eudaimonia* is attained through enacting a virtuous life which revolves around training the emotions and developing rational understandings of how to act in diverse contexts. That said, in virtue ethics there is a focus on the development of character rather than on adjudicating instances of right or wrong action. Therefore, virtue ethics is concerned with questions such as *What is a good life?* or, more specifically, *What does it mean to be a good person?*[47]. This ethical stance holds a commitment to concepts such as excellence, virtue, and *eudaimonia*, instead of those of duty, right, and obligation as expounded in deonotology[48]. A virtuous agent *knows* the correct way to act in various contexts while also *desiring* to act in such a way. In this capacity, evaluations of virtuous character can only be derived accurately as a contextual practice.

By approaching IoT design through a lens of virtue ethics, it is possible to connect with the values-based experiences of designers, engineers, and developers while they work, exploring the negotiations and tacit norms embedded in the making of connected devices as a contextual activity. For example, when designers of IoT technologies debate and disagree about what tools to use and how to manage and respond to data, they are simultaneously enacting a form of ethics. Consciously or not, designers give prominence to and enact certain ethical values through the socio-technical affordances that they attribute to their creations.

A virtue ethics approach can enable understanding of how, when, and where designers and developers make decisions about the technologies they create and to identify potential areas for intervention. Furthermore, examining ethical engagement from this perspective allows us to identify whether or not classical conceptions of the virtues have changed in accordance with the evolution of connected societies. But it would be a mistake to assume that a virtue ethics approach would identify prescriptions required for ideal ethical comportment. More promising for social scientists and ethnographers in particular is Alasdair Macintyre's[49] identification of how virtue ethics can work to highlight the role of social worlds in shaping how people develop ideas of the 'good life' and 'responsibility'. Macintyre's arguments about practical reason stress the significance of an individual's social milieu for the development of their practical

[45] Annas, J. (1993). *The Morality of Happiness*, New York, NY: Oxford University Press.
[46] ibid
[47] Hursthouse, R. (2001). *On Virtue Ethics*. New York, NY: Oxford University Press.
[48] White, R. (2008). *Radical Virtues*. Lanham, MD: Rowman & Littlefield.
[49] MacIntyre, A. (2016). Ethics in the Conflicts of Modernity: An Essay on Desire, Practical Reasoning, and Narrative. Cambridge: Cambridge University Press; MacIntyre, A. (1985). After Virtue, London: Duckworth.

reasoning. He also discusses how practical reasoners from various places and backgrounds engage with the political and moral realities that they encounter.

Identifying the ethical thinking which goes into making connected technologies is essential, because the social contexts that produce them make certain assumptions about the uses of data and the appropriate ways to respond (or not) to the challenges posed by connected objects. In this respect, "virtue ethics provides an integral but open and dynamic framework in which fruitful intercultural dialogue about information technology ethics can take place"[50].

Some early elements of this approach to identifying tensions within social spaces as well as dynamic negotiations of values, self-identified virtues and the virtues that are constructed relationally between individuals and collective contexts. In our work, we seek to identify also how these contexts shape and constrain how flourishing is defined in relation to IoT development.

Our research findings point to at least two things: 1) that the development of IoT represents a conflict about how to use emergent forms of knowledge and associated values, 2) that the values (and virtues) developed and enacted in these connected environments are intimately bound to context in terms of existing social institutions and norms (Tasks 2.1; 2.2). Many of the ways that people expressed values, for example, illustrated how particular forms of knowledge are constrained by particular kinds of social institutions and impact technomoral values that are then reified into concrete ethical principles[51]. These are in turn relational, and although they can be challenged, for example, through the development of manifestos, they are also shaped by the relationships to dominant and influential institutions.

3.6 Enacted Ethics and Development of Field Sites

Certain sites and orientations have consistently appeared as places where people attempted to identify and develop alternative ethical positions – and similar actors continued to appear (Tasks 2.1; 2.2). We have participated in quite a few of these as illustrated in the previously presented overview of all fieldworks conducted so far in the project (including ThingsCon Salons; The IoT Trustmark; the Open IoT Studio Retreat). What is most striking with recurring ethical concerns across sites is that they mobilise a complex interplay between *ethics* and *law*, where applications of laws are viewed as means of addressing ethical issues. For many IoT developers who point to data, privacy, and security as ethical concerns ethics is articulated with words also appearing in laws developers must comply with in their development practices. This articulation is most prominent among developers encountered at the larger IoT conferences where few point to ethical concerns beyond data, privacy

[50] Vallor, S. (2010). Social network technology and the virtues. *Ethics and Information Technology, 12* (2), 157-170.
[51] Vallor, S. (2016). *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*. New York, NY: Oxford University Press

and security when asked openly about what is ethically at stake in development of IoT technologies.

Taking the indication that a conception of ethics in IoT development among some developers appear as tightly connected to matters directly touching upon compliance with laws further, an insight across the visited field sites indicates that the law seems to work as a limit-case for ethics. This is most clearly expressed at events we have been participating in where IoT developers seek to create a space for discussing and reflecting upon ethics in the development of IoT technologies. In these spaces, ethical discussions are moving beyond legal domains and words attached to IoT development in laws as also expressed in the manifestos.

Through events such as ThingsCon Salons, The IoT Trustmark, and the Open IoT Studio Retreat, ethics is enacted as a matter beyond compliance with existing laws through discussions that also occasionally move on legal borders or point towards future laws. Quite a few developers during these events, as well as within specific IoT domains such as sustainability or particular communities such as Arduino, present ideas of ethics in IoT reaching far beyond otherwise commonly shared concerns about privacy, security and data. We will not outline all empirical material supporting these observations, but give a brief example of European communities and a domain introducing or creating space for the introduction of diverse ethical concerns that expand the ethical terrain. These findings highlight the importance of ethical approaches that can account for ethics in practice, and encompass the contradictions in how people express ethics and enact them through design.

When asked to describe ethics in IoT development an Arduino developer responded that ethics is about open source, community, equality in access to services and interactions between people. At the Torino Mini Maker Faire two other members of the Arduino community immediately responded when asked about ethical challenges and possibilities in IoT development: ‘There are a lot of ethical challenges – too many for us!’. Following on from this they equally pointed towards the centrality of community feeding into their vision of an ideal open source scenario in which they describe boards and hardware would be offered for free while trusting that the community gives something back: ‘All the community lives on this particular trade between what you give and what you get […] It’s challenging because today’s world is not doing this. If you see it in a larger view. All the circular economy stuff.’ Hence, asking about ethics in IoT development with these three Arduino members opened up for a very different conversation about ethics than was the case during the bigger IoT conferences.

Another example of this kind of expanded ethical discussion is expressed through conversations with IoT developers working in the domain of sustainability. Both during the Internet of Green Things Festival in Copenhagen and the Torino Mini Maker Faire, IoT developers working with sustainability raised ethical concerns that were not articulated through any of the otherwise recurring concepts like privacy, security and data. A developer at The Internet of Green Things Festival had, for

example, developed a technology to sense whether garbage cans are full or not to reduce CO2 emissions caused by cars driving to pick up garbage even if the bin is not full. He was, however, concerned that this might mean that some people who need this job would be fired in the future. A similar concern was expressed by an IoT developer at the Torino Mini Maker Faire seeking to create a green sensing wall full of plants. He was reflecting upon how 3D printers might steal jobs in IoT developments processes from people who need these jobs. Another developer at the Internet of Green Things Festival was working on an app making water consumption transparent through real time monitoring where 15% of the expenses related to the water you save goes to charity.

A third example of how ethics is enacted beyond dominant concepts attached to ethics and IoT is during ThingsCon Salons where we have attended one in Berlin and hosted one in Copenhagen as part of TechFest 2017. ThingsCon is a global community of practitioners engaging with IoT and it is one of Europe's leading conference networks in this field. ThingsCon wishes to contribute to a movement of practitioners: 'who champion shared values like openness, sharing, diversity & inclusivity, sustainability'[52], as stated on their webpage. ThingsCon wishes to create a responsible and human-centric IoT and through Salons around Europe in a range of cities including Berlin, Amsterdam, Milan, Cologne, Copenhagen, discussions about ethics and responsibility in IoT development are facilitated.

VIRT-EU hosted one such salon where some of the concerns expressed by participants included whether IoT technologies are dangerous? What is the ethical/moral framework attached to IoT technologies? Is something done for the sake of tech rather than real benefit? The intensity and affective tonality during this event in combination with questions as these indicate just how deeply IoT technologies seem to reach into the lives of the diverse group of participants underlining the ethical stakes in IoT development and why these cannot be pinned down to compliance with existing laws and regulations. Another example of ongoing events expressing this challenge are tied to the 'IoT Trustmark' which we describe in the following section. This leads to a synthesis of what insights about ethics in IoT developments participation in these events have brought forward as we present our justification and identification of field sites and informants for in depth fieldwork in the next phase of the project.

[52] see http://thingscon.com/

3.7 Sites for Development of Alternative Governance Frameworks: Open IoTMark

Our fieldwork identified that many manifesto authors and other people interested in using design to find ways to bring forward ethical discussions related to the IoT were also engaged in a community-led, bottom up process to define a trustmark indicating that an IoT device met particular ethical standards. This process began with a large meeting in London in June, where participating developers attempted to create ethical principles for trustworthy IoT technologies. However, upon closer examination, the event also demonstrated how particular kinds of knowledge are constrained by particular kinds of social institutions and impact values that are then reified into concrete ethical principles.

As a response, our research team began to pursue a participatory research strategy, convening a further meeting of participants, and bringing insights from the first round of fieldwork to the community of practice (Tasks 2.1; 2.2; 3.3). We aim to continue engaging with the IoTMark project as one of our detailed field sites exploring the possibility and challenge of exploring ethics in practice (Task 3.3). At the first IoTMark event, held on the five-year anniversary of the Open IoT definition first drafted in 2012[53] industry representatives, software engineers, academics, and lawyers had come together as a global community-led effort to develop a certification mark for connected products (consumer or industrial).

A primary motivation for the community was the desire to seek protections for consumers who were often put at risk because of surreptitious, data-driven business models and unethical design issues. According to members of the community present at the event, there were no natural market or regulatory dynamics (outside of the upcoming GDPR) currently addressing these issues. Although the mark would be voluntary, it would, nevertheless, provide a guideline for ethical practice other than laws. An important concern expressed by one of the participants was that new technologies were giving rise to new challenges which could have serious implications for freedom. With regards to the IoT ecosystem, he flagged the following aspects as key:

- Ensuring reliability in terms of multiple connectivity, mobility, and cost worthiness;
- Ensuring availability of scarce resources;
- Maintaining an open and level playing field;
- Building trust; and
- Supporting the IoT ecosystem.

[53] see http://iot.london/open-internet-of-things-definition

While Trust Mark participants were in agreement with the above, what eventuated by the close of the first day of the event was not a normative shift to incorporate a robust ethics into the design and development of IoT. Rather, what transpired was the constraining of ethics by participants' social milieu, which supports Macintyre's (2016) claim that contextual factors have the potential to influence the development of ethical subjects and ethical thinking. It is perhaps reasonable to conclude that these outcomes were the result of the kinds of voices privileged during the event: male software developers, most of whom were fixed primarily on technical principles.

Following the launch, the document was placed online, participants met weekly through conference calls and discussed particular challenges through ongoing discussion on a Slack channel. Collaborators framed general concerns into a focused set of principles and identified how principles could be operationalised.

The second event (September 11, 2017) was facilitated by Virt-EU researchers from the LSE based on preliminary fieldwork as well as investigators' previous research[54]. Suggestions provided included absorbing other assessment frameworks into the mark (for example, using existing ethical frameworks on privacy as elements of a mark's framework, or explicitly involving a broader range of stakeholders including consumer rights advocates). In the LSE-led session, a smaller group with more female representation worked to develop and operationalise the principles (privacy; interoperability; openness; data governance; permissions and entitlements; transparency; lifecycle, provenance, sustainability & futureproofing) that were to underpin the mark (Task 3.3).

Following this meeting, the IoTMark project hosted a workshop at the Mozilla Festival to refine the principles[55]. The event aimed to identify a set of stakeholders who might be further engaged to take these principles forward, including digital rights organisations and start-ups – and begun to consider how to distinguish this trustmark project from others by embracing a 'progressive interpretation of openness'. Ongoing examination of the editing of the live trustmark documents reveals continued controversy about how to interpret and enact openness, how to balance commercial demands and consumer protection, and how to facilitate broad acceptance of ethical principles without alienating powerful institutional actors (Task 3.3).

3.8 Identification and Justification of Specific Field Sites and Informants

Based on the initial field research presented in the previous section, we note how some European IoT developers seek to create spaces for ethics in IoT development entailing, but simultaneously challenging, dominant concerns about privacy, security and data as encapsulating the stake of ethics. This domain mapping has identified that a focus on these alternative positions, combined with data-driven identification of specific sites for

[54] Powell, A. (2012). Democratizing production through open source knowledge: from open software to open hardware. *Media, Culture & Society, 34* (6), 691-708
[55] see https://iotmark.wordpress.com/principles/mozfest17/

sustained involvement within the most active IoT regional hubs across Europe, provides a strategy for formulating the future engagement with this domain (Tasks 2.1; 2.2).

We propose a continued and sustained engagement within the networks of IoT developers in London and Amsterdam, including continued participation in the IoT mark process and ThingsCon Salons as bottom-up engagements encompassing the development of ethical frameworks by building and sustaining a network of startup-based and design oriented actors. Our ethnographic and participatory research in these fields will generate new insights into the networked connections between grassroots ethical actors across Europe. We will continue to participate in and structure events, as well as linking this research with online network mapping, perhaps through employing Slack and GitHub data[56].

In addition to continuing our fieldwork in these two fields, we will also use network and legal research to support the identification of specific start-up partners who might become sites for long-term ethnographic fieldwork, both within London and Amsterdam and, where necessary, beyond. The framework for this process of surfacing field sites, as developed within our synthesis workshop, is the following:

1. That the qualitative team has evidence from their fieldwork that indicates location likely to have a dense and connected network of developers
2. That the quantitative team has supporting similar evidence from Meet-up
    a. Attendance should be above a certain threshold
    b. Frequency of meet-ups should be more than a (given) number of times per month or year
    c. Topics of meet-up should be diverse (though IOT-focused)
3. To note:
    a. What type of regulation is present in regards to IOT? Hard, soft, or none at all?
    b. What is the type of development occurring primarily? Hardware or software or mixed?
    c. What is the company size?
4. Bonus attributes of a field site location would be:
    a. Advisory board recommends site and shares contacts of developers / companies
    b. Literature identifies the site as having many of the features of 1, 2

3.8.1 London

As the initial fieldwork highlights, IoT innovation and investment emerged strongly in London due to clustered research, civic innovation, and SME industrial contexts (Tasks 2.1; 2.2). As such, London remains a central hub for IoT development, but even more importantly for our project, it remains a central node in many important IoT networks, including research, policy and advocacy. In addition, regular London IoT MeetUps generated network data that allowed the project to identify participants in start-up culture across the city, while large-scale projects such as PETRAS have mapped the

[56] see https://github.com/openiotmark/iotmark-principles

industrial landscape[57]. Many members of the advisory board suggest a continued focus on London as a field site, although some uncertainty emerges related to the local community's response to the introduction of the GDPR given the prospect of the UK leaving the European Union.

3.8.2 Amsterdam

Another central field site in our forthcoming in depth fieldworks is Amsterdam, a geographical space we have not engaged with physically, but which has been strongly present in multiple ways across all the field sites we have entered. We have learned that central figures promoting ethical debate point to, or are strongly connected to, Amsterdam (such as ThingsCon Salons, the IoT Design Manifesto, the Things Network, IoT Council and Dyne.org). These communities of IoT developers offer a possibility to qualitatively enter different engagements in IoT development carried by a variety of contextual values. This is expressed in manifestos authored by participants in the respective communities as well as through conversations with some of these during the outlined ethnographic engagements in the domain mapping. The IoT Meetup environment in Amsterdam is active, facilitating the use of network data to help surface field sites. The engagements seem to move beyond European borders which is valuable in terms of engaging with the networks and circulations of values amongst IoT developers in Europe also from a network perspective (where some participants cut across sites in London and Amsterdam among others).

[57] see https://www.petrashub.org/

4.0 Data Ethics: Legal and Regulatory Aspects of Data Ethics

4.1 Foreword

The main aim of the project concerns the investigation of the ethical and social issues of data use to provide IoT developers with practical guidance to conduct a Privacy, Ethical and Social Impact Assessment (PESIA). In line with this, Polytechnic University of Turin (POLITO) and Open Rights Group (ORG) have conducted initial research on policies and institutional contexts for data identification, collection and analysis in Europe (Task 2.4).

The first months of the project have been devoted to clarifying the research goals on the basis of a literature analysis and, therefore, to define the main research questions with regard to the legal domain. POLITO and ORG started from the following three general research questions based on the Virt-EU project description:

> RQ1: How can ethical and social issues be taken into account in IoT development?
> RQ2: Which ethical and social issues should be taken into account?
> RQ3: How can we facilitate IoT developers in embedding ethical and social values in their products/processes?

After an initial literature review, these questions have been reformulated as follows for the POLITO/ORG team:

> RQ1: How can we go beyond the limits of the existing regulatory framework and take into account ethical and social values?
> RQ2: Which ethical and social issues in data processing are taken into account by DPAs, Article 29 Working Party, European Court of Human Rights, European Court of Justice and privacy practices?
> RQ3: How could the PESIA model facilitate IoT developers in embedding ethical and social values in their products/processes?

To address these questions POLITO and ORG, which compose the research team focused on legal issues, adopted a rough division of the field of their investigation into two areas, on the basis of their different nature and approach.

On the one hand, POLITO Legal & Technology Research Group mainly adopts an academic approach focusing on various issues concerning Law & Technology and therefore focuses on data protection regulation, case law and legal theory. From a methodological perspective, POLITO's investigation considers theoretical as well as

empirical evidence directly collected by POLITO, provided by partners or available in literature.

On the other hand, ORG is an NGO with wider experience in interaction with civil society, regulators and developers, and some experience engaging with ethical frameworks in relation to data. For this reason, ORG's main research goal is to survey the wider regulatory framework around IoT (security, safety, intellectual property, etc.), and analysing the practices adopted by IoT developers, the technical issues concerning the use of data and the existing tools and frameworks available for ethical practices and/or privacy.

Against this background, the task of the POLITO-ORG research team in this project is to identify ethical and social values and render them operational through the development of the PESIA approach, in a manner consistent with data protection principles and the existing regulation (i.e. GDPR). This also characterises the interaction between the POLITO-ORG team and the other partners and their respective research tasks in light of the development of the PESIA model.

The PESIA model is the result of a two-stage co-design process. In the first stage, POLITO-ORG and the other partners focus on empirical investigation (LSE and ITU), collecting empirical results from their respective fields to define the main values for the PESIA model, to be developed by POLITO-ORG (Deliverable D4.3, M24), and validated through co-design (CIID). In the second stage, after M24, the model will be tested in workshops with developers (Task 5.2) and the outcome of these workshops may be used to re-design part of the PESIA or better design the sector-specific PESIA models (Tasks 4.3 and 4.4, Deliverable D4.4).

Regarding POLITO-ORG's initial findings and plans for further research activities in WP4, this first part of the project is necessarily characterised and influenced by the transition from the current EU data protection framework, which is based on Directive 95/46/EC and its national applications, to the new Regulation (EU) 2016/679 (GDPR). In this light, our first 24-month research plan focuses on the following areas:

- Data protection, ethics and the wider regulatory landscape of IoT
- GDPR and ethical and social values
- Ethical and social values in case law and soft-law

The first area (data protection and ethics), which is the object of this section, is the narrowest one and is an introduction to several legal issues that we will address later in the project. This section deals with ethical and social values and mainly concerns data ethics and the rationale of data protection. In addition, this section provides an overview of the policy environment of IoT, including other relevant regulations. This is important to understand any other potential ethical claims or considerations by developers, such as attitudes to product safety or environmental concerns.

4.2 Limits of Regulation and Our Future Research Strategy

From the perspective of the development of the PESIA model, it is important to be aware of the limits of regulation in addressing societal issues. These limits are evident in the transition from the Directive to the new General Data Protection Regulation (hereafter GDPR). For this reason, the first part of the legal analysis carried out in this deliverable, starts from the framework defined in 1995 and still in force.

On the one hand, in the Directive, the EU legislator has tried to satisfy the demand of data subjects to be in control of their data by recognising the prominent role of individual consent and imposing information duties on data controllers. On the other hand, over the years, the "notice and consent" mechanism has been limited in providing an effective safeguard to moral and social values: situations of power imbalance and cognitive limits of data subjects have impaired the effectiveness of the data subject's consent. This is an important element, which should be taken into account in the next deliverables in order to assess whether the GDPR offers new solutions to bolster the data subject's interests and address the issue of collective dimensions of data processing.

In the light of the above, in their second contribution (deliverable D4.1), POLITO and ORG will show how the new regulatory framework does not properly address the criticisms already envisaged during the last years of application of the principles provided by Directive 95/46/EC. More specifically, the data protection impact assessment, as defined in the GDPR, seems not to be able to go beyond the traditional approach in data protection (DPIA/PIA) and to encompass ethical and social values.

Given the limits of the current and future regulatory framework, as well as the need to adopt a broader approach not merely focused on law provisions, in months 12-24 of this project POLITO-ORG's investigation will outline the social and ethical values which assume relevance in data processing. To reach this goal, POLITO will review and analyse different legal sources. The results of this analysis will be used to set the stage for the development of a preliminary model of PESIA. The following stages represent how the investigation conducted by POLITO and ORG will be undertaken:

- Analysis of the decisions adopted to identify the ethical and social values which are taken into account to regulate data use by the following authorities: data protection authorities (Italy, Spain, France, United Kingdom, Belgium, Germany), Article 29 Working Party, European Court of Human Rights, European Court of Justice. The international charters and documents adopted by the International Conference of Data Protection and Privacy Commissioners will also be analysed
- Analysis of the main PIA models and procedures adopted in various countries; analysis of ISO standards
- Analysis of the results of other projects funded by the EU with a focus on risk assessment and data use
- Survey of IoT policy and regulatory environment
- Analysis of developers' privacy practices based on consortium research

- Analysis of available ethical and privacy practical tools and frameworks, ranging from principles to engineering methodologies.
- Analysis of regulations on ethics committees
- Development of the PESIA model (M24)

4.3 Integrating Empirical Perspectives in the Development of PESIA

In the research and evaluation of ethical and social issues regarding the use of data, the VIRT-EU project integrates multiple methodologies, including social network analysis and qualitative analysis of dominant and alternative ethical perspectives.

As described previously, IoT developers encounter ethical and social issues regarding the gathering and processing of personal data that they respond to in different ways.[58] This raises various questions, as demonstrated by several recent cases: is it ethically acceptable that toys register children's conversations?[59] Is it ethically acceptable that wearable devices store information regarding users' health or intimate life? Is it socially acceptable to install default geo-localisation devices in smartphones? Is it socially acceptable reshaping private or public areas through augmented reality?[60]

As a complement to other research, it is important to take into account further sources and quantitative studies to investigate and represent the point of view of European citizens – not only developers – about the use of personal information. This makes it possible to identify the values which are more perceived to be put at risk by data processing.

To such end, this analysis considers the quantitative studies carried out at the European level, such as the Eurobarometer report on data protection[61] and the Eurobarometer report on e-privacy.[62] Since these studies regard all EU citizens, they include a broader perspective than the studies presented above, and outline of the ethical principles and social values that characterise European societies with regard to the use of personal information.

The analysis of the different perspectives is furthermore important, since the interests and values considered by IoT developers, on the one hand, and data subjects, on the

[58] More generally, on the ethical role of technologists, see also Mario Bunge, (1977), 'Towards a Technoethics', 60, 96-107.
[59] The problem emerged with so-called 'smart dolls', which can interact with children users, collect data and send behavioural advertsing: see www.law.kuleuven.be/citip/blog/smart-dolls-a-triple-threat-to-children-and-their-rights. Accessed November 17, 2017. For an empirical analysis on smart toys see Emily MCReynolds, Sarah Hubbard, TomothyTimothy Lau, Aditya Saraf, Maya Cakmak, Fanziska Roesner, 'Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys, (2017) http://dx.doi.org/10.1145/3025453.3025735.http://dx.doi.org/10.1145/3025453.3025735. Accessed November 23, 2017.
60 Pokémon go app, for instance, raises this problem. See Brandon R. Teachout, 'Gotta Collect It All!: Surveillance Law Lessons of *Pokémon Go*' (2016) 69 Stanford Law Review 83.
[61] Special Eurobarometer 431 “Data protection”, released in June 2015.
[62] Flash Eubarometer 443 “E-privacy report”, released in July 2016.

other, may not necessarily coincide, or may be described in different ways as the findings presented above by LSE and ITU illustrate. This includes considerations of not just values that participants claim to observe but those that are put into practice.

The manifestos elaborated by technology developers[63] certainly constitute important documents, but they are not enough to tell us neither which values are effectively put into practice, nor whether these values are consistent with the values commonly accepted by a given society. To this end, we should instead examine how these manifestos are practically enacted.

In order to identify the guidelines concerning the ethical and social values which should drive IoT development, the analysis will therefore start from empirical studies of broad citizen views, which complement the analysis of how values are understood by developers.

To address this challenge, it is necessary to start from the assumption that ethical and social issues as perceived by society underpin the legal dimension of data protection, and that such principles are enacted by legislators when drafting regulations, and by judges and authorities when applying them.[64] Data protection regulation as interpreted in a broad sense (laws, jurisprudence, guidelines, soft-law and practices) can therefore provide us with useful indications regarding the values guiding data processing.

4.3.1 Data Protection as an Ethical and Social Problem

Since the first discussions and proposals concerning data protection regulation, data protection has been drafted to provide an answer to ethical and societal issues concerning the use of data.[65] The right to privacy and the right to the protection of personal information in European case law and literature have been placed in the context of personality and fundamental rights. This is the result of a long development from the theoretical, regulatory, jurisprudential and social perspective, which cannot be discussed in depth in this context.[66] Nevertheless, it is important to outline the main stages of this development, focusing on the social issues which influenced them.

---

[63] On the role of manifestos regarding digital rights, see Engin Isin, Evelyn Ruppert, 'Being Digital Citizens' (2015) 167-179.

[64] On the relationship between virtue ethics and the law, see Nesteruk J. (2017) *Virtue and the Law: Contemporary Perspectives*, in Sison A.J.G., Beabout G.R., Ferrero I (eds.) *Handbook of Virtue Ethics in Business and Management* (Dordrecht: Springer) 847-856. On the role of ethics in the rule of law, see Tallachini M. (2009) Governing by Values. EU Ethics: Soft Tool, Hard Effect. *Minerva*, 47, 281-306.

[65] See Simitis S. (1989) Privacy – An Endless Debate. *California Law Review*, 98, 1989-2006.

[66] See Bygrave L. (2014). Data Privacy Law: An International Perspective (Oxford: Oxford University Press) 8-15; Tzanou M. (2017) The fundamental right to data protection: normative value in the context of counter-terrorism surveillance (Oxford: Hart Publishing); González Fuster G. (2016) Emergence of personal data protection as a fundamental right of the EU (Dordrecht: Springer); Rodotà S. (2009) Data Protection as a Fundamental Right in Gutwirth S., Poullet Y., De Hert P., de Terwangne C. and Nouwt S. (eds.) Reinventing Data Protection? (Dordrecht: Springer), 77–82; Cannataci J.A. (2008) Lex Personalitatis & Technology-driven Law. SCRIPTed, 5(1), 1–6; Stromhölm S. (1967) Right of Privacy and Rights of Personality. A comparative Survey (Norstedt & Soners) 28–31. See also Giesker H. (1905) Das Recht der Privaten an der eigenen Geheimsphäre. Ein Beitrag zu der Lehre von den

4.3.2 The First Generation of Data Protection Regulation: The Social Roots of Data Protection

The precursor of the data protection right can be found in the right to privacy, intended to protect an intimate and private sphere of the individual, in a first stage against the public's curiosity (especially the media), and in a second stage against public authorities. The need to protect individuals from public powers was abruptly called into question during the first half of the 20th century. The possible consequences of the misuse of information, especially for discrimination purposes, emerged with dramatic meaningfulness. A direct consequence of this can be seen in the special attention accorded to data revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership and health or sex life. Privacy emerged not only as an individual issue, but as concerning society at large.

In a sense, data protection regulations have their social roots in the societal consequences of the computer revolution of the late 50's, when the migration from dusty paper archives to computer memories permitted, for the first time, the aggregation of information about every citizen that was previously spread over different archives.[67] Data protection was thus the response to the growing concern of citizens about the risk of computer-based social control by governments[68] and large corporations.[69] Therefore, the notion of data protection was originally based on the idea of control over information,[70] and the first data protection regulations gave individuals a sort of counter-control over collected data.[71] They pursued this goal by increasing the level of transparency about data processing and safeguarding the right to access to information.

Mandatory notification of new databases, registration, licensing procedures and independent authorities were the fundamental elements of these regulations. Another

---

IndividualrechtenIndividualrechten (Zürich: Müller); Kohler J. (1907) Urheberrecht an Schriftwerken und VerlagsrechtVerlagsrecht (Stuttgart: F. Enke) 441.

67 See Secretary's Advisory Committee on Automated Personal Data Systems (1973) Records, Computers and the Rights of Citizens. http://epic.org/privacy/hew1973report/ accessed November 23, 2017.

68 Miller A.R. (1971) The Assault on Privacy Computers, Data Banks, Dossiers (Ann Arbor MI: University of Michigan Press) 54-67; Mayer-Schönberger V. (1997) Generational development of data protection in Europe? in Agre P.E., Rotenberg M. (eds.) Technology and privacy: The new landscape (Cambridge MA: MIT Press) 221-225. See also González Fuster G. (2014) The Emergence of Personal Data Protection as a Fundamental Right of the EU (Cham: Springer International Publishing) 28-36.

69 See Bennett C.J. (1992) Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Ithaca: Cornell University Press) 29-33, 47; Brenton M. (1964) The Privacy Invaders (New York: Coward-McCann); Packard V. (1964) The Naked Society (New York: David McKay). See also U.S. Department of Health, Educatin & Welfare (July 1973) Report of the Secretary's Advisory Committee on Automated Personal Data Systems and Bygrave L.A. (2002) Data Protection Law. Approaching Its Rationale, Logic and Limits (The Hague: Kluwer Law International) 107-112.

70 See Westin A.F. (1970) Privacy and Freedom (New York: Atheneum) 7; Solove D.J. (2008) Understanding Privacy (Cambridge MA: Harvard University Press) 24-29.

71 See U.S. Department of Health, Education & Welfare (July 1973) Report of the Secretary's Advisory Committee on Automated Personal Data Systems. See also Mayer-Schönberger V. (1997) Generational development of data protection in Europe? in Agre P.E. and Rotenberg M. (eds.) Technology and privacy: The new landscape (Cambridge MA: MIT Press) 223.

key component was the right of access, which allows citizens to ask data owners about how information is being used and, consequently, about the exercise of power over information. Finally, the entire picture was completed by the creation of *ad hoc* public authorities to safeguard and enforce citizens' rights.

4.3.3 The Second Generation of Data Protection Regulation: The Notion of Self-Determination Based on Individual Consent

This scenario changed in the mid 80s, when in many cases the big mainframe computers were superseded by personal computers at a relatively low cost. Consequently, computational capacity was no longer an exclusive privilege of governments and big companies, but became accessible to many entities and consumers.

This period witnessed another transformation involving direct marketing: new forms of marketing based on customer profiling and extensive data collection took place; information was no longer collected to support supply chains, logistics and orders, but to target products at specific users. As a result, the data subject became the focus of the process and personal information acquired economic and business value.

These changes in the technological and business frameworks led legislators to face new demands from society, since citizens wanted to have the chance to negotiate their personal data and gain something in return. Although the new generations of the European data protection laws placed personal information within the context of fundamental rights,[72] the main goal of these regulations was to pursue economic interests related to the free flow of personal data,[73] even though the European approach was, and remains, less market-oriented than other legal systems.

Both the theoretical model of fundamental rights, based on self-determination, and the rising data-driven economy highlighted the importance of users' consent in consumer data processing. Consent does not only represent an expression of choice with regard to the use of personality rights by third parties, but it is also an instrument to negotiate the economic value of personal information. Moreover, effective self-determination in

[72] See Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 28 January 1981 and entered into force on 1st October 1985 httphttps://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (accessed November 23, 2017); OECD, Annex to the Recommendation of the Council of 23rd September 1980: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#preface (accessed November 23, 2017). See also González Fuster G. (2014*) The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Cham: Springer International Publishing) 163-205 and 253-272; Tzanou M. (2013) Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *IDPL*, 3(2), 88-99; Rodotà S. (2009) *Data Protection as a Fundamental Right* in Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds.) *Reinventing Data Protection?* (Berlin: Springer) 77–82.

[73] Directive 95/46/EC. See also Poullet Y. (2006) EU data protection policy. The Directive 95/46/EC: Ten years after. *CLSR*, 22(3), 206; Simitis S. (1995) From the Market to the Polis: The EU Directive on the Protection of Personal Data. *Iowa Law Review*, 80, 445.

data processing, both in terms of protection and economic exploitation of personality rights, cannot be obtained without adequate and prior notice. For this reason, the "notice and consent" model[74] added a new layer to the previous paradigm based on transparency and access.

In the light of the above, Directive 95/46/EC represents both the general framework and the synthesis of this second wave of data protection laws,[75] which have their roots in a technological and social scenario in which information, under the form of data, is processed in an increasingly efficient manner and in larger amounts, not only quantitatively, but also from a qualitative point of view.

4.3.4 Big Data and IoT: Toward a Change of Paradigm?

The present ability to collect, retrieve and analyse large amounts of data, thanks to the development of cloud computing and big data analytics,[76] makes it possible to monitor social behaviours, infer patterns of behaviour and apply such patterns to individuals in order to predict their actions and therefore take decisions affecting them. Such computational power belongs not only to public authorities, but also to private actors, to whom the traditional checks and balances system used to restrain public power could not apply.

The impact of such a computational revolution is magnified by the diffusion of devices that make extensive data collection possible and put large amounts of information in data silos owned by private or public companies, which are able to use these data to find new correlations and extract further information.

Moreover, in the last few years, the number of devices that allow data collection has exponentially increased: from computers and tablets to smartphones, from appliances to wearable devices. This phenomenon is referred to as the Internet of Things (IoT), indicating that objects used for daily purposes are able to collect data and eventually transmit it through a web, thus allowing further processing.[77] IoT therefore allows more

[76] On the big data revolution see Tene O., Polonetsky J. (2012) Privacy in the Age of Big Data: A Time for Big Decisions. Stanford Law Review Online, 64, 63-69; Rubinstein I.S. (2013) BigData: The End of Privacy or a New Beginning. International Data Privacy Law, 3(2), 74-87; Richards N.C., Jonathan H., King J.H. (2014) Big data ethics. Wake Forest Law Review, 397-405; Mayer-Schöenberger V., Cukier K. (2013) Big Data: A Revolution That Will Trasform How We Live, Work ans Think (New York: Houghton Mifflin Harcourt); Krasnow Waterman K., Bruening P. (2014) Big Data Analytics: Risks and Responsibilities. International Data Privacy Law, 4(2), 89-95. See also Bollier D. (2010) The Promise and Peril of Big Data https://www.emc.com/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf accessed November 23, 2017; Council of Europe (2017) Guidelines on the protection of individuals with regard to the processing of personal data in a word of Big Data https://rm.coe.int/16806ebe7a accessed November 23, 2017; McKinsey Global Institute (2011) Big data: The next frontier for innovation, competition, and productivity https://bigdatawg.nist.gov/pdf/MGI_big_data_full_report.pdf accessed November 23, 2017 .

[77] On the notion of IoT and the issues it arises, see Weber R.H. (2010) Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26, 23-30; Atzori L., Iera A., Morabito G. (2010) The Internet of Things: A survey. *Computer Networks*, 54(15), 2787-2803; Popescul D.,

intrusive collection of data, in contexts, such as private houses, which are usually considered part of a protected sphere of the individual, whose activities are registered without any active intervention from the data subject.[78] The more IoT pervades objects which are commonly used for everyday activities, the more it is difficult to avoid data collection.

The individual cannot help but leave behind her a trace of data. Technology gives the possibility to collect such data in intrusive ways, especially by monitoring individual activities. It is then possible to analyse large amounts of data and extract further information (so-called data mining): for example, by monitoring Internet browsing activity, the data controller can infer habits, preferences and aptitudes of the data subject. Individuals are then profiled in different categories, which can lead to discriminatory practices.[79]

Technology developments allow such processing, but is it always ethically and socially acceptable to do so? Data protection law aims at addressing this question by providing a framework that is responsive to the societal needs regarding the values which should drive the future algorithmic society. In this sense, not only data protection regulations partially embed ethical principles, but they can also provide a more harmonised context in which different contributions of different components of our societies (e.g. IoT developers, industry, consumers, local and national governments, etc.) can be encompassed through different participatory models.

4.4 Relevant Ethical Aspects

Although, as briefly outlined in the previous paragraph, ethical values have largely inspired data protection regulation and have been partially embedded in it, legal frameworks – intentionally or unintentionally – do not cover all the ethical issues concerning data use. This is due to two main reasons: on the one hand, the limits of regulatory and jurisprudential remedies to promptly follow and adopt societal changes; on the other, the intention to leave room for flexibility avoiding a codification of ethical or social values.

Georgescu M. (2013) Internet of Things – Some Ethical Issues. *The USV Annals of Economics and Public Administration*, 13-2(18), 208-213; Peppet S.R. (2014) Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent. *Texas Law Review*, 93, 117-146; Thierer A.D. (2015) The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. *Richmond Journal of Law & Technology*, 21(2), 4-17, 53-63.

[78] See Crabtree A., Mortier R. (2017) *Personal Data, Privacy and the Internet of Things: The Shifting Locus of Agency and Control*, unpublished https://doi.org/10.13140/rg.2.2.34496.12809, 2, who notes that the IoT reshapes "the nature of data collection form ad 'active' feature of human-computer interaction to a 'passive' one in which devices seamlessly communicate personal data to one another across computer networks".

[79] See Hildebrandt M. (2006) Profiling: From Data to Knowledge. The challenges of a crucial technology. *Datenschutz und Datensicherheit*, 30(9), 548-549; Schermer B.W. (2011) The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27, 46-50.; Schermer B.W. (2013) *Risks of Profiling and the Limits of Data Protection Law* in Custers B., Calders T., Schermer B., Zarsky T. (eds.) *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Berlin Heidelberg: Springer-Verlag) 138-140.

From this perspective, and in light of the main goal of the Virt-EU project (i.e. providing guidance to IoT developers concerning ethical and social values), the research conducted in WP 2 - Task 2.4 has outlined the most relevant aspects and tasks of data ethics, as stemming from empirical research and from the data protection framework.

Data ethics has emerged from computer and information ethics as a new branch of ethics which studies the ethical problems connected with the use of data, independently from the technological means involved.[80] We should here mean ethical problems in their broader significance, as moral and social issues which need to be addressed to make choices and orient human behaviour. More specifically, the aim of the Virt-EU project is to analyse how ethical (and social) issues should be taken into account by IoT developers to perform their tasks in an ethically acceptable way.

Therefore, from this perspective, it is important to better investigate the role played by data ethics through the lens of its interplay with law and society. For this reason, it is essential to identify the circumstances in which ethical issues arise and, secondly, the values to be protected.[81]

4.4.1 Ethical Aspects Regarding Data Collection and Data Use

Regarding the first aspect, ethical problems concern the generation and collection of data in itself. Is it ethically acceptable that so much personal data is created in the first place? What are the circumstances which justify the traceability of data that individuals leave behind them? Are there ways to collect data which are more acceptable than others? Another set of issues regards the concentration of power which comes with data collection. The value of data relies not only on the computational capacity to process data in order to extract valuable information, but also upon the availability of large amounts of data. As a consequence, it comes that data gatherers are interested in collecting huge quantities of data. This raises serious ethical issues regarding the concentration of power held by few subjects, both private and public, which have the

---

[80] Floridi L., Taddeo M. (2016) What is data ethics?. *Phil. Trans. R. Soc.*, 374(2083) http://dx.doi.org/10.1098/rsta.2016.0360 accessed November 23, 2017, who define data ethics as “the branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing, and use), algorithms (including AI, artificial agents, machine learning, and robots), and corresponding practices (including responsible innovation, programming, hacking, and professional codes)”; European Data Protection Supervisor (2015) Opinion 4/2015 'Towards a new digital ethics https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf. Accessed November 23, 2017.

81 See the approach adopted by the Information Accountability Foundation (2015) Unified Ethical Frame for Big Data Analysis, part A, 7-10 http://informationaccountability.org/wp-content/uploads/IAF-Unified-Ethical-Frame.pdf. Accessed November 23, 2017, which identifies five key values (beneficial, progressive, sustainable, respectful, fair) to help define the important questions for an ethical code with respect to big data.

capacity to collect and process big data.[82] Those subjects do not operate in the IoT sector only; instead, this phenomenon crosses over different fields and involves market actors who offer goods and services which are not necessarily connected to IoT.

Ethical problems also concern the use of data. Under this perspective, the scope and purposes for which data are processed come into question. We must therefore assess the ethical evaluation having regard to the goals of data processing in each single case. Different values are concerned, if, for example, data are processed for scientific research or for marketing purposes.

The technologies used to process data are also to be taken into consideration when comparing ethical issues. In this sense, the different uses of algorithms are receiving particular attention, since algorithms mediate social processes and base decisions taken both by private actors and public authorities, without (or with limited) human intervention. The case of algorithms clearly demonstrates that technology in itself is not neutral, but may carry the biases of its creators. Hence, ethical problems must be addressed ahead of data processing, when designing the technologies that will be used to manage data.

The collection and processing of personal data can finally pose delicate ethical issues when specific categories of data are involved (such as data relating to vulnerable sectors of the population, children, for example, or data relating to health conditions) or when there is an imbalance of power between the data subject and the data controller.[83]
Identifying Ethical Values: Individual and Collective Values

Against this background and in order to guide IoT developers in the collection and processing of data, data ethics must also identify the underpinning values to be used as evaluative criteria.[84] In fact, data ethics investigates the limits within which data gathering and processing are morally and socially acceptable. These values originate

[82] See also Zuboff S. (2015) Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89; Andrejevic M. (2014) Big Data, Big Questions|: The Big Data Divide' *International Journal of Communication*, 8, 1673–1689; Mantelero A. (2014) Social Control, Transparency, and Participation in the Big Data World. *Journal of Internet Law*, April, 23-29; Mantelero, A., Vaciago G. (2013) The "Dark Side" of Big Data: Private and Public Interaction in Social Surveillance, How data collections by private entities affect governmental social control and how the EU reform on data protection responds. *Computer Law Review International*, 14(6), 161-169; Boyd D., Crawford K. (2012) Provocations for a cultural, technological, and scholarly phenomenon. *Journal Information, Communication & Society*, 15(5), 662-679.

[83] The Working Party art. 29 takes into consideration the imbalance of power between the parties when assessing the prerequisite of freedom of consent. See WP29 (2011) Opinion on consent 5/2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf. Accessed November 23, 2017, 13, where it excludes that consent is freely given if the data subject is under the influence of the data controller, such as in an employment relationship or, in general, when the refusal to consent could give rise to negative consequences. On the asymmetries in data negotiations when big data is involved, see Mantelero A. (2014) The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. *Computer Law & Security Review*, 30, 654-659.

[84] On the notion of values see Spiekermann S. (2016) *Ethical IT Innovation* (Boca Raton; London; New York: CRC Press) 39-44.

from society and, in many cases, are codified by law. Moreover, they inspire various charters of fundamental rights and freedoms and are enacted by judicial decisions.

In this light, data protection regulation, whose focus is on data uses, represents an attempt to frame the different values involved and strike a balance between competing interests. Data subjects' interests may differ from services providers' interests. For example, data subjects might be interested in their online activity not being monitored, while service providers may want to track users in order to obtain valuable information. Therefore, data protection regulation and its concrete applications can provide an important contribution in identifying and balancing the interests and values involved in each case.

Traditionally, data protection derives its roots from the need to preserve an intimate and private sphere of the individual, who is given the remedy of excluding others from such sphere. This perspective sees personal data as an attachment of the person: the digital persona, who is made of all the information which the person (mostly accidentally) creates. Thus the person is entitled to the right to informational privacy, intended as the right to control her information.[85]

This is a right shaped around traditional personality rights and, in particular, around the right to privacy, which extends its content to protect all information relating to the individual. Hence, personal data can be collected and processed only if the data subjects have given their consent and within its limits.[86] Individual control of personal data is aimed at protecting certain values, such as privacy, identity, reputation and dignity. The intrusiveness of IoT puts at risk such values, as it allows service providers to monitor individuals in their private life and to use the data collected in such way to profile and infer further information about users.

Empirical studies show the importance of ethical values but also illustrate the limits of frameworks like individual consent. As the research conducted by ITU and London School of Economics in WP3 (Task 3.3), privacy (as informational privacy) is an important value to IoT developers. Likewise, the Data Protection Eurobarometer found that a majority of respondents are concerned about not having complete control over the information they provide online and deem it necessary that data controllers obtain explicit approval before processing data. Therefore, there is a clear perception of the need to maintain control over personal information.

[85] It is well known that the right to informational self-determination was first affirmed by the German Federal Constitutional Court in 1983 in the National Census Case: Volkszählungsurteil, 65 BverfGE 1, 68-69 (1983); in this decision, however, the Court considered the individual right to informational self-determination as a precondition to exercise all constitutional rights, therefore protecting not only the individual, but the democratic structure of the State. On such right see Rouvroy A., Poullet Y. (2009) *The Right to informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, in Gutwirth S., Poullet Y, De Hert P., de Terwangne C., Nouwt S. (eds.) *Reinventing Data Protection?* (Heidelberg: Springer) 45-76.

[86] Exemplary of this approach is the work of Westin A. (1967) *Privacy and Freedom*.

However, it is worth noting that the role of individual consent to protect informational privacy has been contested, since consent does not always ensure that the individual is actually aware of what she is consenting to or even of the fact that she is giving consent.[87] In this light, the protection of individual rights must not rely on consent only, but data ethics should ensure that, regardless if consent has been given, personal information is processed in a manner consistent with the values accepted by society and without prejudice to the rights and freedoms of the individual.[88]

Moreover, the values which must be considered when assessing the ethical dimension of data, not only refer to the individual, but also regard groups of people or general interests.[89] Discriminatory practices based on data collection, for example, have negative effects not only toward the person who is discriminated, but also to the whole group that is classified in a certain manner.[90] In these cases, the role of individual consent is restricted, as the values involved go beyond the person individually considered. Moreover, individuals may have a limited perception of the general or collective interests impaired by data processing.

---

[87] This applies especially if data controllers ask for consent using long privacy statements which users do not usually read: this is the so-called "transparency paradox". See Nissenbaum H. (2011) A Contextual Approach to Privacy Online. *Daedalus*, 4, 32-48. See also Rubinstein I.S. (2013) Big Data: The End of Privacy or a New Beginning?. *International Data Privacy Law*, 3(2), 74; Brandimarte L., Acquisti A., and Loewenstein G. (2010) *Misplaced Confidences: Privacy and the Control Paradox*, Ninth Annual Workshop on the Economics of Information Security http://www.heinz.cmu.edu/~acquisti/papers/acquisti-SPPS.pdf accessed November 23, 2017; Turow J., Hoofnagle C.J., Mulligan D.K., and Good N. (2007) The Federal Trade Commission and Consumer Privacy in the Coming Decade. *ISJLP*, 3, 723-749 http://scholarship.law.berkeley.edu/facpubs/935 accessed November 23, 2017; Federal Trade Commission (2014) *Data brokers. A Call for Transparency and Accountability*, http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf accessed November 23, 2017, 42. On the limits of the traditional notices, see also Calo R.M. (2013) Against Notice Skepticism in Privacy (and Elsewhere). *Notre Dame L. Rev.*, 87(3), 1027, 1050-1055 http://scholarship.law.nd.edu/ndlr/vol87/iss3/3 accessed November 23, 2017; Solove D.J. (2013) Privacy Self-management and The Consent Dilemma. *Harvard Law Review*, 126, 1880, 1883-1888; World Economic Forum (2013) *Unlocking the Value of Personal Data: From Collection to Usage*, http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf. Accessed 2014.November 23, 2017, 18. For an overview on the relevant research see Solove D.J. (2013) Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126, 1883-1893.

[88] See Richards N.C., King J.H. (2014) Big data ethics. *Wake Forest Law Rev*., 409-413, who suggest intending privacy as information rules, not necessarily relying on consent. In the same direction, though in the different context of online behavioural advertising, see Tene O., Polonetsky J. (2012) To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioural Advertising. *Minn. J. L. Sci. & Tech*., *13* (1), 347.

[89] Mantelero A. (2016) Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law & Security Rev*., 32, 238-255

[90] Collective and general interests are put at risk not only by the use of personal data (i.e., data referred to an identifiable person), but by the use of data, even if anonymised: Barocas S., Nissenbaum H. (2014) *Big Data's End Run around Anonimity and Consent* in Lane J., Stodden V., Bender S., Nissenbaum H. (eds.), *Privacy, Big Data, and the Public Good* (New York: Cambridge University Press) 45; Jacob Metcalf J., Kate Crawford K. (January-June 2016) Where are human subjects in Big Data research? The emerging ethics divide. *Big Data and Society*, 11. Anonymisation itself has been criticised as not guaranteeing against re-identification: in this sense, see Ohm P. (2010) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization'. *UCLA Law Review*, 57, 1701.

Finally, the values and interests underpinning the protection of personal data must be confronted with the interests of those who want to collect and process data. Circulation of information must also be protected, as it can serve purposes, which are not only ethically acceptable, but also socially desirable (for example, scientific research). Data ethics serves to select such purposes and identify the procedures to process data when pursuing such ends. Hence, data ethics is called not only to identify the values involved, but also to strike a balance in case those values are in conflict. Nevertheless, it may be problematic to identify shared values in situations where there is not a strong consensus on ethical issues.

This may also be the consequence of data processing activities, which are usually a-territorial. Since they do not occur in one specific place, but involve controllers and data subjects from different States and communities, it will not always be possible to identify a shared data ethics. In such cases, it is necessary to adopt a pluralistic approach and consider the specific ethical values of the different groups involved.

4.5 Data Ethics and the Law

Both regulators and civil society actors express an urgency that data processing follows ethical guidelines and stress the fact that ethics needs to go beyond the law[91]. In fact, data ethics can go beyond the law in requiring IoT developers to take into consideration data subjects' values to a larger extent than what is strictly required by law. We can see the importance of this when technology evolves more rapidly than the law, thus making insufficient the safeguards put in place by the latter.

In other cases, law is not enough to ensure ethical behaviours regardless of technological evolution. For instance, the rule which requires consent as a legitimate basis for data processing does not guarantee that it is always ethical to process data even if consent has been given. In many cases, the consent requirement may represent only a formal safeguard against risks arising from data processing, especially if it is required in situations characterised by a strong imbalance of power between the data subject and the controller. However, this does not mean that the law cannot be a source of moral and social values. Actually, the juridical order can refer to social rules, which, in turn, integrate the former.

Such integration clearly takes place when the law itself refers to social and moral values through general clauses. In this sense, general clauses are principles posed by legislators, which refer to social and moral evaluations. For instance, data protection law provides that data can be processed without obtaining the data subject's consent if there is a legitimate interest of the controller, which is not "overridden by the interests or

[91] European Data Protection Supervisor (2015, 11 September) *Opinion 4/2015 'Towards a new digital ethics'*; The Information Accountability Foundation (2017, 20 September) *Artificial Intelligence, Ethics and Enhanced Data Stewardship*, 1. See also Richards N.C., King J.H. (2014) Big data ethics. *Wake Forest Law Rev*., 429, who underline the limits of the law in times of rapid technological change.

fundamental rights and freedoms of the data subject".[92] The notion of legitimate interest is therefore not specified by the law, which only makes some examples and gives some criteria. Does it constitute a legitimate interest to process data for market surveys? We can also pose the question as: is it ethical to process data for market surveys without the data subject's consent? Which safeguards must be observed?

4.5.1 The Role of General Clauses

The presence of a general clause means that written law does not give a direct answer to such ethical problems, but refers to more general principles, which can also be derived from society.

Another important example is the clause of necessity and proportionality in the use of data, which underpins data protection regulation. In other words, the processing must be limited to what is necessary to its scope, and must be proportionate considering the underlying interests and values. The principle of necessity and proportionality could, for example, restrict the use of airport body scanners if it is not strictly justified by public interests.

While the law refers to proportionality, a need for reasonableness seems to emerge from the empirical research among IoT developers: it appears to be commonplace the reference to a reasonable standard to assess data collection. As long as reasonableness is referred to the purposes of data processing, it seems very close to the necessity and proportionality principles as outlined by data protection regulation. In this respect, a self-assessment tool such as PESIA could guide technology developers to put reasonableness into practice, giving them a tool to evaluate when a certain data processing is to be deemed reasonable.

Finally, the clause of fairness is another general clause which clearly refers to moral and socially shared values and conducts: data must be fairly processed. Also in this case, to assess what fairness is, we need to investigate what is socially considered fair from a moral point of view.

4.6 Application and Interpretation of Legal Norms

A further form of integration between written law and social and moral dimensions takes place when the law is interpreted and applied. Rules, which are general and abstract, must be adapted to specific cases. Such process is usually carried out by judges and, in the case of data protection, by supervisory authorities as well.

In this respect, there are cases in which some rules require a higher degree of judicial intervention in order to narrow their scope and be applied: consider, for example, the prescription to carry out the data protection impact assessment when the processing "is likely to result in a high risk to the rights and freedoms of natural persons".[93] In order to

[92] Art. 6, para. 1, lett. f), Reg. 679/2016/EU; art. 7, lett. e, Directive 46/95/CE.
[93] Art. 35, para. 1, Reg. 679/2016/EU.

apply such rule, it is necessary, on a preliminary basis, to enucleate the values to be protected and balance them with competing interests.

Consider, also, the rule which requires “freely” given consent to the processing of personal data: here, again, the law does not specify what free consent is, but only offers some criteria.[94] Is it lawful to develop a business model in which the user has no choice but to consent if she wants to access the service, or should alternative options be given? Would consent be deemed free in such circumstances? To give an answer to such questions, interpreters and judges inevitably take into consideration the moral and social implications and consequences of their decisions.

More generally, data protection law must be interpreted considering the rights protected by the EU Charter of Fundamental Rights, which explicitly recognises the right to the protection of personal data.[95] This is clearly a very elastic interpretation, which allows moral and social values to step in.

In conclusion, there are many cases in which the law itself does not provide for strict rules, but leaves space to discretional applications, which must be anchored to moral and social evaluations. Here data ethics clearly serves to integrate the law, therefore it is possible to infer ethical guidelines by analysing how the law is applied.

Against this background, data ethics should not be considered in contrast to the law. On the contrary, ethics serves to integrate the law, which *per se* already takes into account several moral and social values. In other words, law rests on a substratum of moral and social values, which shape data protection regulation.

For these reasons, when looking for ethical principles, the project will also investigate how data protection law is applied in practice through a complex mix of regulatory tools, such as judicial and supervisory authorities' decisions. The analysis of this regulatory mix should contribute to revealing the ethical and social values that should guide developers in their most crucial decisions.

4.7 Empirical Analysis

As we have seen, the Virt-EU project intends to draw ethical and social values from empirical observation. Since it is not possible to assume that the legal scenario can provide a complete picture of moral and social values existing in our society, a relevant element of the investigation carried out by POLITO concerns the analysis of the empirical evidence provided by the qualitative research conducted by the LSE team and the existing quantitative studies.

[94] On such requirement see Article 29 Data Protection Working Party (2011, 13 July) *Opinion 15/2011 on the definition of consent*, 12-17.
[95] Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, *6* (2), 77.

In carrying out this part of the project, it is important to consider the values as perceived from all the different actors and stakeholders involved in data processing and not to leave any relevant interests and expectations out. Other sections of this report cover in detail the perspectives of people involved in developing IoT technologies, but it is also important to consider the results of studies regarding both data subjects and data controllers. For this reason, the following sections analyse the data subjects' and developers' points of view, on the basis of both quantitative and qualitative empirical evidence.

4.7.1 The Data Subjects' Point of View

In order to derive some insights on the data subjects' point of view from a European perspective, which considers the differences existing among the various national communities, this empirical analysis evidence is based on the 2015 Eurobarometer on Data Protection and on the 2016 Flash Eurobarometer on e-Privacy. These studies refer to European citizens and, as such, include data controllers and technology developers alike, but do not consider the latter as separate categories. Instead, these surveys aim at analysing the perception of privacy issues under the data subjects' perspective.

Since the results from these surveys refer, as mentioned, to European citizens, it must be taken into account that they may largely vary according to nationality (and, of course, to other factors, such as age and level of education, as well as the consequence of a different legal framework in terms of data protection).[96] However, this does not diminish the relevance of these findings: on the contrary, it is in line with the context-based nature of the social and ethical values that represent the focus of the Virt-EU project. From a general perspective, the main finding of these survey concerns the relevance of data protection *per se* as a value and the framing of this value as a form of control on personal information by the data subject.[97] The nature of this value is consistent with the main accepted legal notion of data protection,[98] which is actually the result of ethological studies,[99] confirming the interplay between society and law, at the origins as it is nowadays.

---

[96] On such issue regarding European surveys on privacy and data protection, see Hallinan D., Friedewald M., McCarthy P. (2012) Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, 28, 264. On how cultural differences can affect privacy perceptions, see PRISMS, (The PrIvacy and Security Mirrors: Towards a European framework for integrated decision making), Deliverable 7.1:Report on Existing Surveys, 176-178.

[97] On the value given to privacy by individuals, see Acquisti A., John L.K., Loewenstein G. (2013) What is privacy worth? *Journal of Legal Studies*, 42, 267-270; Bauer C., Korunovska J., Spiekermann S. (2012) On the Value of Information – What Facebook Users are Willing to Pay. *ECIS 2012 Proceedings*, paper 197, 11-13. See also Solove D.J. (2013) Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126, 1883-1893, who underlines the limits of privacy self-management by individuals. On empirical studies regarding public attitudes toward privacy, see PRISMS (The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making), Deliverable 7.1:Report on Existing Surveys, 14 March 2013,125-127.

[98] See Solove D.J. (2008) *Understanding Privacy* (Cambridge, MA: Harvard University Press).

[99] Westin A. (1970) *Privacy and Freedom* (New York: Atheneum).

Regarding the value of protecting personal information, European citizens do not feel to be in control over their personal information[100] and this situation represents an issue for them. Indeed, a large majority of respondents (67%) is concerned about not having complete control.[101]

To address this problem, many respondents think that data are to be collected and processed only with the data subject's permission. In particular, European citizens affirm that it is important that the information stored on devices (such as computers, smartphones and tablets) is accessed with permission and that online activities are monitored with consent.[102] More generally, they oppose information being shared without consent and think that explicit approval is always necessary to manage personal data.[103]

Moreover, European citizens want to be informed about what happens with their data, and, particularly, if their information happens to be lost or stolen[104].
The surveys also point to the ineffectiveness of the traditional tools provided for by the legislator to address the problem of data control, that is to mandate data controllers to inform data subjects of the collection and further processing of their data. This is done by means of privacy statements (privacy notice), but only a minority of respondents read them.[105]
The reasons of such attitude are of different nature: respondents say that privacy statements are too long and difficult to read; that they have scarce confidence that they will in any case be complied with; that they trust the law to protect them in any case; that they do not deem it important to read the full terms or simply cannot find them. This

[100] According to Special Eurobarometer 431, only 15% of respondents say they have complete control over the information they provide online, while 31% think they have no control at all. Partial control over data is felt by 50% of respondents.
[101] Special Eurobarometer 431, 12. Special Eurobarometer 431, 12. See also the results of the survey conducted in August 2017 by Mozilla, '10 Fascinating Things We Learned When We Asked The World 'How Connected Are You?' https://blog.mozilla.org/blog/2017/11/01/10-fascinating-things-we-learned-when-we-asked-the-world-how-connected-are-you/. Accessed November 23, 2017.
[102] Respectively, 92% and 82% according to Flash Eurobarometer 443, 29.
[103] Respectively, 71% (Flash Eurobarometer 443, 55) and 69% (Special Eurobarometer 431, 58).
[104] 91% according to Special Eurobarometer 431, 72.
[105] According to Special Eurobarometer 431, 84, 18% of respondents fully read privacy statements, 49% partially read them and 31% never read them. These results are confirmed by other studies: see Nissenbaum H. (2010) *Privacy in context* (Stanford: Stanford University Press) 105; Milne G.R., Culnan M.J. (2004) Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. *Journal of interactive Marketing*, 20-21. This can be seen in the broader context of the so called 'privacy paradox', by which individuals concerns about privacy do not match their actual behaviours: Spiekermann S., Grossklags J., Berendt B. (2001) E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behaviour. *Proceedings of the 3rd ACM Conference on Electronic Commerce* (New York) 28-47; Norberg P.A., Horne D.R., Horne D.A. (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41(1), 100–126. See also the results of the survey conducted in August 2017 by Mozilla, '10 Fascinating Things We Learned When We Asked The World 'How Connected Are You?' https://blog.mozilla.org/blog/2017/11/01/10-fascinating-things-we-learned-when-we-asked-the-world-how-connected-are-you/. Accessed November 23, 2017, which found that, even though losing privacy is a main concern, privacy (and security) are not top concerns for people shopping for connected products.

results in only a minority of respondents (mainly young or better educated people) being always informed about data processing.[106]

European citizens also seem not to actively exercise their right to access to information, as demonstrated by the few requests received by data controllers.[107] On the other hand, data subjects seem more active in adopting different solutions to avoid data collection.[108] In this sense, a majority of respondents affirm they have changed internet browser privacy settings,[109] while others use software to prevent being monitored. More drastically, not being in control leads a large part of European citizens to avoid certain websites for fears of being monitored.

Not only is control on personal information valued, European citizens are also concerned about having to disclose their data in the first place,[110] although there is a widespread perception that disclosure of personal data is somewhat inevitable and is part of modern life.[111] In spite of this, the majority of respondents say that providing personal information is an issue for them and they worry about having to provide their data in return for free services.[112] In the same light, a large majority finds it unacceptable that their online activity is monitored in return for unrestricted access to a website and that they have to pay in order not to be monitored.[113] Younger generations are less concerned about the disclosure of their data than older people.

The surveys also provide us with useful insight concerning the reasons why European citizens want to be in control of their data.[114] First, there are some specific risks that European citizens fear in case they lose control of their personal information: the most common one is the use of online identity for fraudulent purposes. The use of data for direct marketing and risks regarding personal safety are the second threats.[115]

---

[106] According to Special Eurobarometer 431, 81, only 20% of respondents is always informed about data processing, 41% is sometimes informed, 22% rarely and 11% never.

[107] According to Flash Eurobarometer 226, 34, 45% of companies received access requests and only 6% received more than 50 requests in one year (declining from 2003); only 3% received complaints from data subjects.

[108] See also PRISMS, Deliverable 7.1: Report on Existing Surveys, 127-129.

[109] Respectively, 60%, 27% and 40%, according to Flash Eurobarometer 443, 36.

[110] See also Strickland L.S., Hunt L.E. (2005) Technology, Security and individual Privacy: New Tools, New Threats, and New Public Perceptions. *Journal of the American Society for Information Science and Technology*, 229, whose empirical studies reveal a widespread distrust against RFID and smart cards in the US.

[111] According to Special Eurobarometer 431, 28, 71% of respondents say it in part of modern life and 58% that it is inevitable to obtain products or services.

[112] Respectively, 57% and 52%: Special Eurobarometer 431, 38.

[113] Respectively, 64% and 71%: Special Eurobarometer 431, 55.

[114] On the costs of disclosing data, from the data subjects' point of view, see Acquisti A. (2010) *The Economics of Personal Data and the Economics of Privacy*, http://repository.cmu.edu/heinzworks/332/. Accessed November 23, 2007, 15-17.

[115] According to Special Eurobarometer 431, 100, 40% of respondents fear fraudulent uses of their data, 19% fear direct marketing and 18% fear risks to their persona safety: See Phelps J.E., D'Souza G., Nowak G.J. (2001) Antecedents and consequences of consumer privacy concerns: an empirical investigation. *Journal of Interactive Marketing*, 15, 10-15, who investigates the interrelationships between consumers' attitudes toward direct marketing and privacy concerns.

Unsolicited commercial calls are also perceived as inconvenient.[116] Only a small minority of respondents fear that data processing can lead to reputation damage, discrimination practices and misunderstandings.[117]

Second, respondents seem to worry not about specific risks stemming from data processing, but about the fact in itself of not being in control of their information. Indeed, they are worried that information is used without their knowledge, stolen, shared with third parties without their consent, used in different contexts from what was authorised, or lost.[118]

Thus, it seems that the notion of privacy as felt by European citizens it that of *informational privacy*, i.e. the right of the data subject to be in control of her data.[119] It also seems that respondents are not fully aware of the potential risks posed by data processing to society at large, such as discrimination or societal control. Instead, they tend to focus on risks taking place at an individual level, such as fraudulent uses of data.[120] Finally, the surveys address the perception of responsibility and trust in data protection.

As regards the responsibility to ensure that data provided online are safely processed, a large majority of respondents say that responsibility is shared between online companies and individuals themselves.[121] In part, this is coherent with the importance accorded to individual control on personal data and to individual consent: if consent is necessary to process data, then the individuals are responsible for the protection of their information. To a slightly lesser degree, public authorities are also considered responsible.[122]

4.7.2 Trust in Data Controllers

However, European citizens do not fully trust data controllers.[123] In particular, online businesses are the least trusted (only 24% trust them), while health and medical

116 61% of respondents say that there are too many unsolicited commercial calls: Flash Eurobarometer 443, 50.
117 Respectively, 7%, 5% and 5%: Special Eurobarometer 431, 100.
118 Respectively, 32%, 29%, 25%, 20% and 8%: Special Eurobarometer 431, 100.
119 On the different types of privacy that emerge from empirical studies, see PRISMS (The PrIvacy and Security Mirrors: Towards a European framework for integrated decision making), Deliverable 9.1: Findings from qualitative focus group, 29 October 2013, 36.
120 In this sense, see Hallinan D., Friedewald M., McCarthy P. (2012) Citizens' perceptions of data protection and privacy in Europe. *Computer Law Sec. Rev.*, 28(3), 265, 268; SAPIENT (Suporting fundamental rights, Privacy and Ethics in surveillance Technologies), Final Report, 25 July 2014, 8.
121 67% of respondents say online companies are responsible and 66% that individuals are: Special Eurobarometer 431, 104. Similar results emerge from PRISMS, Deliverable 9.1: Findings from qualitative focus group, 37.
122 55% of respondents think that public authorities are responsible: Special Eurobarometer 431, 104.
123 The subject of trust was also studied by the EINS Project (Network of Excellence in Internet Science), see in particular deliverable D5.1.2: Internet Privacy, Identity, Trust and Reputation Mechanisms, 13.1.2014, http://www.internet-science.eu/publication/822. See also PRISMS, Deliverable 7.1: Report on Existing Surveys, 129-130. These results are confirmed by a survey conducted by the Information and Commissioner's Office (6 November 2017) Trust and confidence in data,

institutions and national public authorities are the most trusted.[124] A large part of respondents also trusts banks and financial institutions and European institutions[125]. Instead, only a minority trusts shops and stores and phone companies and Internet services providers.[126]

The results of the Eurobarometer surveys have been substantially confirmed by a study conducted by the European Commission on the governance of IoT,[127] which, as we shall see, also support initial ethnographic findings from Virt-EU. According to the survey on IoT, these new technologies are seen by a large majority of European citizens as bringing significant economic and social benefits, but also posing numerous ethical problems, "including the sense of personal identity, individuals' autonomy, user consent, fairness and social justice".[128]

With this in mind, it is possible to observe how the perceptions of data subjects do not coincide with those of IoT developers. While the majority of respondents affirm the need to safeguard user consent and user control regarding personal data in the IoT context, some industry players argued that explicit consent will not always be achievable.[129]

Moreover, European citizens do not seem to trust IoT developers to appropriately self-regulate themselves regarding the development of IoT, but call for a strong regulatory framework to protect individuals' rights and autonomy. On the contrary, industry players stress the role of the market and think that the current legal framework is enough.[130]

These main findings confirm, from an empirical perspective, that the protection of personal data an important issue for European citizens, who want to be in control of their data. At the same time, they also point to a problem of trust, meaning that European citizens do not have much confidence that data controllers will protect their

---

http://www.comresglobal.com/polls/information-commissioners-office-trust-and-confidence-in-data/, according to which only a fifth of UK public report having trust and confidence in companies and organisations storing their personal information; also consistent with the Eurobarometer survey is the result that the UK public are more likely to trust public bodies rather than private companies or organisations.

124 Respectively, 74% and 66% of respondents trust them: Special Eurobarometer 431, 63. Regarding trust in state institutions, see Hallinan D., Friedewald M., McCarthy P. (2012) Citizens' perceptions of data protection and privacy in Europe. Computer Law Sec. Rev., 28(3), 267, who underline that "whilst there seems to be a belief that institutions will try to behave in the right way, there is far a lower belief that in their capability to control and safeguard the data they have been given". The situation seems to be different in the US, where there is a widespread distrust of public authorities as regards data protection: see Ponemon Institute (30 June 2010) Privacy Trust Study of the United States Government, http://www.privacylives.com/wp-content/uploads/2010/07/ponemon-2010-privacy-trust-study-of-us-govt-06302010.pdf. Accessed November 23, 2017.

125 Respectively, 46% and 51%: Special Eurobarometer 431, 63.

126 Respectively, 40% and 31%: Special Eurobarometer 431, 63.

127 European Commission, Report on the public consultation on IoT governance, 16/01/2013.

128 European Commission, Report on the public consultation on IoT governance, 8.

129 European Commission, Report on the public consultation on IoT governance, 8.

130 European Commission, Report on the public consultation on IoT governance, 3, 9.

information. This could have an adverse impact on the market if consumers stopped using certain devices because of privacy concerns.[131]

Finally, these surveys underline the ineffectiveness of privacy statements mandated by law to address the issue of data control, as the data subjects scarcely read them.

4.7.3 The Data Controllers' Point of View

On the side of data controllers, we analyse the 2008 Eurobarometer on Data controllers' perception, also in relation to the dominant perspectives on control of data surfaced in the Virt-EU ethnographic domain mapping. Regarding the manner in which data protection regulation is perceived among data controllers, there does not seem to be a very high awareness of the legislation. Roughly half of the Eurobarometer respondents claim to be somewhat familiar with data protection legislation and only a minority (13%) says to be very familiar with it.[132]

In spite of this, a large majority (91%) of respondents recognise that legislative requirements regarding the protection of personal information are necessary, while only a minority says that the law is too strict and think that it is necessary in certain sectors only.[133] Concerning the level of protection granted by data protection law, roughly half the respondents qualify it as medium.[134] However, the majority of respondents do not think that legislation will be able to cope with the increasing of information being shared.

Compliance does not seem to be very high as well. Only half the respondents make use of privacy enhancing technologies,[135] while almost one third does not use them even if they know what they are, and a minority (14%) has never heard of them.[136] Less than half maintain a privacy policy notice.[137] With regard to the transfer of personal data, a third of those who transfer data via the Internet do not adopt any security measure and do not know what standard contractual clauses (which are one of the necessary requirements to transfer data to non EU countries) are.[138] Generally, bigger companies are more aware of and more compliant with the law than smaller ones.

---

[131] See Awad N.F., Krishnan M.S. (2006) The personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quaterly*, *30* (1), 19.
[132] Flash Eurobarometer 226, 9.
[133] Respectively, 35% and 28%: Flash Eurobarometer 226, 15.
[134] 56% of respondents qualify the level of protection as medium, 28% as high and 11% as low: Flash Eurobarometer 226, 10.
[135] On privacy enhancing technologies see European Commission (2007) Promoting Data Protection by Privacy Enhancing Technologies (PETs)', COM(2007) 228 final (Brussels), where PETs are defined as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system".
[136] Flash Eurobarometer 226, 24.
[137] 41%: Flash Eurobarometer 226, 36.
[138] Flash Eurobarometer 226, 26, 32.

With regards to criticalities of the data protection regulation, a large majority of data controllers favour more harmonised rules, further clarifications of the law and a better balance between data protection rights and freedom of expression and information. Moreover, roughly half of respondents favour sector-specific regulation.[139]

The ethnographic domain mapping undertaken by Virt-EU also suggests that IoT developers seem to be struggling at making sense of national and European data protection regulation. Particularly, smaller companies find it more difficult, due to economic restraints, to fully understand and comply with the law. The GDPR, which imposes further burdens and requirements, such as the data protection officer and the privacy impact assessment, increases these issues.[140]

Technology developers seem to perceive data protection law as imposing formalistic requirements and apparently do not understand the moral and social stances that underpin data protection regulation.[141] In this light, tools which are mandated by law in order to make data controllers take into account the impact of data processing (such as the privacy impact assessment) risk being implemented (if they are) in a formalistic way, simply in order to avoid legal sanctions.

Developers often discuss informational privacy as a key ethical value. However, when confronted with practical issues, technology developers do not seem to be able to give this value a stable consistency, linking it with generic concepts such as reasonableness, which is not further explored.

Another critical issue is the local dimension of these values, since the notion of values and privacy might differ in different States, communities or cultural groups. This implies that any assessment tool should, to a certain extent, consider this local dimension, giving voice to communities, which may contribute to co-designing the range of values to be adopted in the tool.

Moreover, among developers, privacy does not necessarily have the same meaning as intended by data subjects. For instance, some IoT developers do not seem to take freedom from behavioural advertising seriously, whereas data subjects feel uncomfortable with companies using their data to tailor marketing techniques. Along the same lines, while data subjects highly value self-determination (thus, the possibility of being in control of their data), many IoT developers taking a dominant perspective on

[139] Flash Eurobarometer 226, 41.

[140] On the challenges in complying with GDPR, see the findings of the survey conducted in September-October 2017 by IAPP and TrustArc, 'Getting to GDPR Compliance; Risk Evaluation and Strategies for Mitigation', https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf. Accessed November 23, 2017.

[141] See also Bamberger K.A., Mulligan D.K. (2015) *Privacy on the Ground: Driving Corporate Behaviour in the United States and Europe* (MIT Press), 227, whose qualitative research conducted among corporate professionals identified as leading in the field of privacy protection in the United States and Europe, shows that, while in Germany corporate approaches to data protection are also driven by socio-ethical concerns (with results similar to those emerged in the US), in France and Spain privacy programs seem to be more oriented toward the law.

privacy in relation to market value do not seem to have put in place mechanisms to safeguard a set of values personalised by the user.

Many IoT developers taking a dominant view of privacy in relation to market benefit view privacy as an asset to be exploited for marketing purposes, meaning that being privacy compliant can increase trust, thus attract consumers.[142]

With regards to the risks posed by data processing, IoT developers do discuss safety and security concerns, in certain sectors in particular (for instance, safety is more highly perceived in IoT domains such as health, automotive and industrial). This may be the consequence of the existing regulatory framework, which is stronger in certain sectors, but it also confirms the decision assumed in this project to develop sector-specific PESIA models which should complement the general model expected by M24.

Regarding security, some IoT developers feel it as a cost which can be sacrificed if it is not economically or financially convenient. Security, as privacy, is also perceived as something that gives companies a competitive advantage on the market and is valued as long as it serves such purposes.

Other risks, such as discrimination, seem to be overlooked in many cases. One of the interviews clearly shows the point. A start-up created an app which was being sold to large companies in order to contextualise customer habits and enable to determine whether the user was a safe or dangerous driver, leading to potential discrimination risks especially in case the data were sold to insurance companies. However, the start-up did not seem to be concerned about such risks.

One of the factors at the base of such low level of awareness concerning the risks posed by data processing might also be that IoT developers seem to discharge responsibility of data protection to the companies which buy and make use of the technologies they develop. Software developers tend to claim that if the product were to cause harm, liability rests on the manufacturer of the hardware and not with the software development. This also demonstrates that technology developers are not fully aware of legal duties and responsibilities regarding the safety of consumers' products.

Finally, qualitative domain mapping research underlines the emergence of manifestos regarding ethical values in IoT. As already noted, manifestos, while demonstrating a certain degree of awareness of ethical problems, do not, by themselves, prove that such ethical concerns are effectively put into practice when developing technology. Instead, they show that IoT developers' communities have a need to formalise ethical problems in written documents and give them consistency. Therefore, there is a need for shared practical guidance when tackling ethical issues.

Both the quantitative and qualitative studies herein analysed demonstrate that data controllers and IoT developers, while claiming at a very general level that privacy and

[142] See Tsai J.Y., Egelman S., Cranor L., Acquisti A. (2011) The Effect of Online Privacy information on Purchasing Behaviour: An Experimental Study. *Information Systems Research*, *22* (2), 266.

data protection are values to be considered, do not spontaneously adopt an ethical attitude. On the contrary, they seem to be more market-oriented, as privacy and data protection are seen as tools to promote consumers' trust. Moreover, legal compliance is seen as imposing formalistic requirements and does not, by itself, necessarily spur ethical behaviours.

The scenario shows the need to elaborate a tool, such as PESIA, which IoT developers can see as a competitive instrument to promote consumers' trust. This, in turn, can foster ethical attitudes and promote a culture of awareness of the social and moral impacts of data processing, thus benefiting both data subjects and technology developers. More broadly, ethical awareness can lead to a higher level of spontaneous law compliance, not only with regard to data protection, but also in contiguous sectors, such as products' safety.

4.8 Regulatory Analysis

The empirical analysis conducted so far shows that there might be, at a very general level, a common framework of values regarding data protection. The need to protect the privacy of individuals and to ensure data control is expressed as a concern both by data subjects and data controllers. However, this perception varies among different stakeholders.

Data subjects seem to have a strong need to be in control of their own data and are concerned about the collection of their personal information. They express a need for consent prior to processing of data and that data gathering be limited. Nevertheless, there is a tension between this need to be in control and the limits of the data subjects' consent. This tension could be overcome by a more articulated and transparent approach intended to increase both the ethically/socially oriented default setting of IoT devices, and the awareness of data subjects' decisions.

On the other hand, many technology developers, while claiming that data protection is important, in practice seem to mainly consider privacy and data protection as tools to increase consumers' trust in order to gain market advantage. Moreover, when data protection collides with economic interests (for instance, if data protection measures are too costly), the latter override the former.

This shows that different stakeholders might not always share common social and moral values, especially when general principles such as privacy and data protection need to be translated into more specific guidelines. From this perspective, the legal framework and its regulatory mix (i.e. data protection legislation, judicial decisions, guidelines, charters of values, best practices and standards) may represent a favourable environment to harmonise those tensions. In this sense, the fact that the data protection legal framework originates from social and moral problems facilitates this role of synthesis of diverse interests and attitudes. A role which may be fostered by a participatory approach in setting common values.

4.8.1 The Regulatory Framework

In many cases, also among developers, there is a positivistic idea of law, largely focused on legal provisions, which undermines the complexity of the legal environment, the heterogeneous nature of the regulatory mix (i.e. data protection legislation, judicial decisions, guidelines, charters of values, best practices and standards), and the constant interplay between law and society.

This does not mean that, mainly in the civil law context, laws do not play an important role in addressing social issues and balancing the different interests existing in society. This is furthermore evident in the European Union law, where the aim to harmonise different regulatory approaches, as well as the necessity to mediate between different stakeholders' interests and pressure groups, make the regulatory framework more open to various societal issues than characterised by a top-down approach.

Moreover, this purpose of harmonising different national regulations has led EU legislators to adopt a flexible approach and strengthen common values. In this sense, EU directives set general principles, giving each member State the task to implement them in a manner consistent with the local regulations and values. In several cases, such as in the field of data protection, the implementation of EU rules adopts a co-regulatory approach which involves, at a national level, both hard and soft law.

On the other hand, EU regulations, which directly apply in member States without having to be enacted by national legislators, are a step further towards harmonisation and may represent a sort of codification of best practices, jurisprudence and guidelines, as well as a compromise between different interests. Thus, for example, the GDPR provides official recognition to the Binding Corporate Rules,[143] codifies the right to be forgotten[144] and lowers the age threshold of data subject's consent consistently with the model adopted by the major social network services.[145]

Regarding data protection, the first attempt to regulate and harmonise European laws has been carried out through Directive 95/46/EC (Data Protection Directive), while a second step has been the recent adoption of Regulation 2016/679 (General Data Protection Regulation or GDPR), which will be applicable starting from May 2018.

Moreover, at the European level, the EU is not the only supranational body to play an active role in defining the regulatory mix. Mainly in the field of data protection, it is also necessary to consider the role of the Council of Europe, a regional organisation promoting the adoption of international conventions. Indeed, the Council of Europe preceded the EU in promoting data protection regulation, setting forth the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention no. 108).

[143] Art. 47.
[144] Art. 17.
[145] Art. 8.

The Council of Europe adopts a regulatory approach that differs from the EU model: the main goal of the Convention is to set a minimum common standard among the Parties.[146] The Convention is therefore a "simple, concise and technologically neutral instrument".[147] This simple nature and the principle-based approach adopted by the Council of Europe, represent the main distinction between Convention 108 and Regulation (EU) 2016/679, where the latter defines a long and detailed set of provisions.

The Council of Europe maintains the original model adopted in the '70s and '80s (e.g. FIPPs, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), which is based on key principles, guidelines and *ad hoc* frameworks. Therefore, the regulatory model adopted by the Council of Europe combines a more flexible principle-based framework with specific guidelines (e.g. the recent Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data)[148] which may be drafted on the basis of a discussion that involves the representatives of different stakeholders.

Not only hard law, but also, and even more, jurisprudence may represent a tool to take into account social dynamics. In this sense, case law is an essential part of the regulatory mix, as it is only through the decision of practical cases that the law is actually enacted.[149] Such enactment is not a strict and formal process but is embedded with social values.[150]

The importance of judicial decisions particularly emerges when hard law does not dictate strict rules, but open principles. This is often the case with fundamental rights charters. As we will see, the recognition of data protection as a fundamental right has originated from and, in turn, has spurred judicial intervention in outlining its scope.

When examining judicial decisions, we should take into account not only courts' rulings, but also administrative bodies' decisions, such as independent authorities. In particular, the Data Protection Directive provides for the establishment of national supervisory

---

[146] See also Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981, https://rm.coe.int/16800ca434. Accessed Novermber 20, 2017, para 20.

147 Kierkegaard S., Waters N., Greenleaf G., Bygrave L.A., Lloyd I., Saxby S. (2011) 30 years on – The review of the Council of Europe Data Protection Convention 108. *Computer Law & Security Review*, *27* (3), 223, 224.

[148] The Guidelines are available at <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a>. See also Mantelero A. (2017) Regulating Big Data. The guidelines of the Council of Europe in the context of the European data protection framework. *Comp. Law & Sec. Rev.*, *33* (5), 584-602.

[149] Judicial authorities operate at both a national and a supranational level. Supranational bodies are able to play a very important role of harmonisation of the law: the European Court of Justice, for instance, ensures that EU law is uniformly interpreted across member States. The European Court of Human Rights (established within the Council of Europe) has a similar function with regards to the European Convention of Human Rights.

[150] See above para. 5.

authorities, which are responsible for monitoring the application of data protection national legislations in each member State.

Finally, in line with the mentioned co-regulatory approach, soft law may complement regulations adopted by EU, international bodies or national legislators. Soft law refers to a variety of instruments adopted by public authorities and private bodies, which are not binding but are nonetheless able to orient behaviour, such as guidelines, recommendations, papers, opinions, self-regulatory tools, codes of conduct, standards.

Soft law can be adopted in an heteronomous manner, by public bodies or private organisations, which propose suggestions and recommendations. For instance, the OECD invited Member countries to implement and disseminate the “Guidelines governing the protection of privacy and transborder flows of personal data”. Indeed, there are institutions whose main function is to issue non-binding opinions; one of these is the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (established by art. 29 of the Data Protection Directive), whose advisory function is aimed at harmonising and clarifying the interpretation of data protection regulation across member States.

Soft law can also be adopted autonomously by the same subjects it aims to regulate. In this sense, soft law is made of self-regulatory tools such as codes of conduct, certifications, declarations and best practices. Stakeholders' practices are thus formalised into written statements or procedures. There can also be private bodies in charge of the observance and enactment of self-regulation, such as ethical committees.

For these reasons, soft law is a clear example of the social dimension of the law: its observance and efficacy do not rest on binding force, but on the shared values and interests it represents. Societal and moral values constitute the direct substratum of soft law, which, in turn, shapes the evolution and interpretation of hard law.

Law must therefore be intended as comprehensive of all such regulatory tools (the so-called regulatory mix), as they are all called to mediate competing interests and, in doing so, channel moral and social values.

4.8.2 The Data Protection Directive

The aim of analysing the data protection regulation is, on the one hand, to extract social and moral values to be taken into account in the processing of personal data and, on the other hand, to verify the impact of the regulation on social practices and perceptions. To such end, the present analysis shall adopt an empirical approach and examine how law is enacted in practice.

In order to do so, the initial investigation of the regulatory framework needs to start from the Data Protection Directive, which represents the cornerstone of European data protection regulation, and not from the GDPR. Moreover, from a structural point of view, the Directive is still in force, whilst the GDPR will apply starting from May 2018.

The Directive currently represents the legal basis of member States data protection legislations, which have not yet been totally replaced by GDPR-compliant regulation. Thus, the Directive represents the current model of European data protection, which has indeed evolved around the Directive.[151]

Furthermore, if we want to take an empirical approach, thus studying a broad array of regulatory tools and not just hard law, we need to take into account the enactment of data protection regulation. Such enactment has only taken place with regard to the Directive. The GDPR is not yet applicable and, in any case, it will take a long time before a significant body of judicial decisions and soft law instruments enacting the GDPR emerges. Therefore, if we limited our analysis to the GDPR only, we would miss the basis of the broader regulatory framework, which is currently built on the Directive.

Finally, as the course of the project shall demonstrate, the GDPR adopts the same values and principles underlying the Data Protection Directive. In terms of values, the relationship between the Directive and the GDPR is that of continuity, not of fracture.[152]

Given the broader regulatory framework in which the Directive is set, we will not enter the details of the Data Protection Directive, but only examine the aspects regarding the impact of data processing on individuals and society and the societal and ethical dimension of privacy and data protection.

The Directive represents the first EU data protection regulation, but is not the first attempt to regulate the subject: The Directive follows the footprints of previous Convention no. 108[153] adopted by the Council of Europe and builds on existing data protection national laws.[154] However, the adoption of a directive is clearly a step forward, as it leads to a greater harmonisation.

The Directive was adopted in the context of the "first pillar" (i.e. the European Community) devised by the Treaty of the European Union, aimed at creating an internal common market. One of the goals was to facilitate the free flow of information across member States, removing the obstacles deriving from differences in national

[151] De Hert P., Papakostantinou V. (2012) The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*, *28* (2), 130, who affirm that "[i]n practice, the Directive has by now become the international data protection metric against which data protection adequacy is measured."

[152] Hustinx P.J. (2013) *(Future) interaction between data protection authorities and national human rights institutione*, in Wouters J., Meuwissen K. (eds.) *National Human Rights Institutions in Europe – Comparative, European and International Perspectives* (Cambridge: Intersentia), 157-1728.

[153] See recital (11) of the Data Protection Directive, which states that "the principles of the protection of the rights and freedom of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data."

[154] The German federal state of Hessen was the first one to adopt a data protection regulation in 1970. It was followed by Sweden in 1973 and Austria, Denmark, France and Norway in 1978. On such laws see Gloria González Fuster, 'The Emergence of Personal Data Protection as a Fundamental Right' (2014 Springer) 56-69.

regulations. This constitutes an important aspect when examining the values and interests underpinning data protection regulation, as it indicates that among them there is also (and not necessarily in a recessive position) the interest of data controllers to process data due to the competitive advantage that data processing entails. It is however important to note that the European legislator considers the relevance of market values in order to create a competitive market which favours not only the industry, but also European citizens and consumers.

On the other hand, the Directive protects the rights and freedoms of the individuals, including the right to privacy.[155] Therefore, the competing interests of data subjects and data controllers already revealed by empirical surveys, emerge in the legislation as well. In this sense, the Directive is actually a result of broader social inputs and it is important to analyse how it has mediated such interests from the point of view of the values involved.

The Directive clearly aims at engaging citizens and society in data processing using different tools. In this light, transparency obligations, data subject's consent and rights of access to information should be briefly mentioned. Moreover, these are all provisions meant to increase the data subject's control over her personal data, which, as emerges from empirical surveys, represents a serious issue among European citizens. Regarding transparency, this is one of the main values protected by the Directive.[156] Transparency is referred to data processing and entails the right of the data subject to know if and which operations are taking place on her data. Data processing must therefore be conducted in a fair[157] and transparent way, so as to give data subjects full understanding of what is happening with their information. Transparency is a prerequisite for the data subject to control her information and to exercise her rights of access.

Transparency also constitutes the basis of the data controller's duty to inform data subjects[158] about who collects and processes their data, for which purposes and how the data are collected and what the data subjects' rights are.[159] The Directive also aims

[155] On the relationship between the right to privacy and the right to data protection, see PRISMS (The PrIvacy and Security Mirrors: Towards a European framework for integrated decision making,), Deliverable 5.1: Discussion paper on legal approaches to security, privacy and personal data protection, 3 February 2013, 13-15; Gellert R., Gutwirth S. (2013) The legal construction of privacy and data protection. *Computer Law & Security Review*, 29, 524-526; De Hert P., Gutwirth S. (2003) *Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence*, in *Security and privacy for the citizen in the post-September 11 digital age: a prospective overview*, IPTS Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE).

[156] On transparency, see González Fuster G. (2014) How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection. *Revista de Internet, Derecho y Política*, *19*, 92-104.

[157] On fairness in data processing see Kuczerawy A., Coudert F. (2011) *Privacy Settings in Social Networks: Is It Fair?* in S. Fischer-Hübner S. et al. (eds.) *Privacy and Identity Management for Life* 6th IFIP AICT 352 (Heidelbert: Springer), 237-238.

[158] Articles 10 and 11 of the Directive prescribe the information to be given to the data subject.

[159] See European Commission (2010) *A comprehensive approach on personal data protection in the European Union*, Brussels 4.11.2010 COM(2010) 609 final, 6, which underlines that the mere provision

at ensuring the data subject's control over her information through the "notice and consent" mechanism. Individual consent, even though it does not constitute the only legitimate ground for processing, is given a central place. The Directive specifies that consent must be specific, unambiguous, free and informed.

The law thus recognises the value of individual control over personal data, which translates into the need to obtain the data subject's consent if there is no another legitimate basis for processing. In order for individual control on personal data to be more effective, the Directive recognises that a data subject possesses a set of rights of access.[160] In particular, the data subject has the right to know whether her data has been collected and processed, for which purposes, by whom and by which means. Moreover, the data subject has the right to obtain rectification, erasure or blocking of data, if the data has been processed without complying with the Directive.

In this aspect, the Directive differentiates itself from previous instruments such as the Convention n. 108 and the OECD Guidelines, which, while prescribing the right of access, did not give such a central role to individual consent. The Directive thus recognises both the economic value of personal data and their personal dimension, and emphasises the role of the individual in consenting the collection and processing of information, provided that transparency is granted.

Under the perspective adopted by the VIRT-EU project, the most important contribution of the Data Protection Directive is related to its capacity to foster awareness of ethical and societal issues relating to data processing. In this capacity, the Directive must be considered against a broader background of other regulatory tools, which have opened data protection to moral and social values and have made society more aware of the individual and collective consequences of data processing. From this perspective, the Directive can be seen as an instrument to contribute to the creation of a European ethics regarding data processing.

The Directive has spurred a series of soft law initiatives which, as we have seen, open the door to a less rigid relationship between law and society at large. In this context, the Article 29 Working Party has played a central role. Its opinions both reflect and shape a

---

that information be given to the data subject is not enough to ensure transparency, as information should also "be easily accessible and easy to understand", and that vulnerable categories such as children deserve special protection. On such communication, see González Fuster G. (2014) How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection. *Revista de Internet, Derecho y Política*, 19, 97, who argues that "[w]hereas transparency had been traditionally understood as a principle implied in the principle of fair processing, encompassing a series of substantive requirements applicable to the data controller's duty to inform, it started then to acquire and additional sense, primarily concerned with the form in which information is to be delivered to data subjects."

[160] On the rights of access, see Raphaël G., Gutwirth S. (2012) *Citizens access to information: the data subject's rights of access and information: a controller's perspective* in PRESCIENT, Deliverable 3, *'Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data*; Galetta A., De Hert P. (2017) *A European perspective on data protection and access rights*, in IRISS (Increasing Resilience in Surveillance Societies), Deliverable 5: Exercising Democratic Rights Under Surveillance Regimes, 5-8 http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysis-Final1.pdf. Accessed November 23, 2017, 5-8.

common European perception of data protection and contribute to the harmonisation of shared values across member States with a focus on specific devices or applications.

The opinions of the Working Party are aimed at addressing challenging ethical issues regarding data protection for which the law does not provide rigid solutions. In addressing these issues, the Working Party has a practical approach, as it does not limit itself to express values and principles, but enacts them giving practical examples on how to balance competing interests.

In this sense, the opinions adopted by the Working Party have mainly the nature of guidance to data controllers and, therefore, represent a kind of document that, compared to law provisions or DPAs decisions, leaves more room to ethical or social considerations.[161] Moreover, the European dimension of this body overcomes the limits of the local/national dimensions and actively contributes in outlining a common ethical framework.

One further recent step in this direction has been the set-up of an Ethics Advisory Group within the EDPS,[162] with the objective to explore the ethical dimension of data protection. This initiative must be considered in light of the increasing relevance that the EDPS has attributed to data ethics in order to protect human dignity and address the new strains posed by technology.[163] From a broader perspective, the Directive is also part of a wider process to consider data protection as a fundamental right.

This is a process which started before the Directive was adopted, due to the judicial interpretation of art. 8 of the European Convention of Human Rights regarding the right to the respect for private and family life.[164] Such a right has been interpreted by the European Court of Human Rights as embedding the right to data protection.[165]

The Directive entered the process, stating that the object of data protection regulation is also to protect fundamental rights and freedoms, notably the right to privacy.[166] Finally, the Charter of Fundamental Rights of the European Union, which entered into force by

[161] See, for example, WP29 (16 September 2014) Opinion 8/2014 on the Recent Developments on the Internet of Things,; WP29 (4 April 2011) Opinion 12/2011 on smart metering; WP29 (19 January 2005) Working document on data protection issues related to RFID technology.
[162] EDPS decision of 3 December 2015 establishing an external advisory group on the ethical dimensions of data protection ('the Ethics Advisory Group').
[163]EDPS (11 September 2015) Opinion 4/2015 Towards a new digital ethics: Data, dignity and technology', 4.
[164] Art. 8, par. 1 states that “Everyone has the right to respect for his private and family life, his home and his correspondence”.
[165] See, for instance, ECHR, Klass and others v. Germany, no. 5029/71, 6 September 1978; ECHR, Malone v. United Kingdom, no. 8691/79, 2 August 1984; ECHR, Rotaru v. Romania, no. 28341/95, 4 May 2000; ECHR, Copland v. United Kingdom, no. 62617/00, 3, April 2007; ECHR, Uzun v. Germany, no. 35623/05, 2 September 2010.
[166] See recital 11 of the Directive.

virtue of the Lisbon Treaty, explicitly recognises the right to the protection of personal data.[167]

The recognition of data protection as a fundamental right represents an important opportunity for moral and social evaluations to enter the law discourse,[168] as it implies the use of general principles, the content of which is not strictly dictated by the law. Also in this sense, the Directive represents a contribution to an increased awareness of the moral and social implications of data protection by society at large, on both sides of data controllers and data subjects.

4.9 First Conclusions and Further Investigation

Against these positive outcomes of the Directive, the findings of the activities conducted during these first months (Tasks 2.4 and 4.1) confirm the relevance of the initial research questions:

> RQ1: How can ethical and social issues be taken into account in IoT development?
> RQ3: How can we facilitate IoT developers in embedding ethical and social values in their products/processes?

These two questions focus on the processes used to operationalise values in the developers' context, in a manner consistent with the broader range of values accepted in our society. They do not concern the question of which values should underpin the PESIA model, but the necessity in itself to adopt this model.

In a context where the legal framework were satisfactory, such questions would be rhetorical: indeed, law would already provide adequate answers. However, the preliminary findings of the legal investigation point out that the regulatory model developed in 1995 and still in force today is only partially adequate to satisfy these issues.

On the one hand, the existing regulatory mix in the field of data protection provides an architecture which is open to social issues; on the other hand, the adopted legal solutions seem to have a limited impact on both developers and citizens at large, in terms of building an effective value-oriented environment.

Nevertheless, under the Virt-EU project perspective, an interesting finding concerns the fact that data protection is considered as a value *per se* and not only as a driver of other

[167] Art. 8 of the European Charter of Fundamental Rights: "Protection of personal data. 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject by an independent authority."
[168] See ECJ, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, 13 May 2014; ECHR Bărbulescu v. Romania, no. 61496/08, 12 January 2016.

ethical and social values. In this sense, European citizens claim greater control over their data and the use of personal information, not necessarily in terms of legal safeguards, but as a social and ethical demand.

In the same way some IoT developers, who, compared to users, often express different and in some cases opposed interests in terms of data uses, consider privacy as a value *per se* (at least on paper). This is indirectly confirmed by their lack of awareness with regard to the legal constraints regarding data protection: this means that data protection and privacy are perceived more as social/ethical values rather than as regulatory mandatory conditions.

Research also suggests that IoT developers are mostly interested in market competitiveness, rather than in data ethics. They also see law compliance as a mere formality in order to not incur sanctions rather than a way to enact ethical behaviour.

Also, smaller developers seem worried by the costs which compliance with GDPR will entail. Concerning law compliance, some of them are not aware of the existing regulations. This happens not only with regard to data protection law, but in other areas as well: for example, software developers are not always aware that, under EU law, they are responsible for the damages caused by their products even if they are incorporated in other devices or are sold by other subjects.

In addition, to be competitive, IoT developers seem to take into particular account security and consumer trust. In this light, PESIA may represent a precious tool to use market competitiveness to increase ethical awareness on data protection issues.[169] As the Eurobarometer shows, a majority of EU citizens do not feel in control of their data and consider this circumstance as problematic. Hence, there is a great need to increase consumers' trust regarding the protection of their personal data and to respond to perceived worries. [170] Technology developers who go in this direction could have a strong appeal on the market.

Technologies designed to protect data can indeed ensure stronger security, also regarding the protection of data subjects' rights and thus gain their trust. This would have beneficial effects for both IoT developers, who would have a stronger market appeal, and data subjects, whose rights would receive enhanced protection. The fact that PESIA, differently to the Privacy Impact Assessment (PIA), is not mandatory could also contribute to its perception not as a mere formality, but as a true substantial ethical assessment.

Against this background, it seems that the general perception of privacy and data protection issues have not found an adequate manner to be expressed and channelled

[169] Mantelero A. (2013) Competitive Value of Data Protection: The Impact of Data Protection Regulation on On-Line Behaviour. *International Data Privacy Law*, 229-238.
[170] Laura Brandimarte B., Alessandro Acquisti A., George Loewenstein G. (2012) Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, *4* (3), 340-347, who demonstrate that increasing individuals' perceived control over their information increases their willingness to share data.

in practical terms. On the one hand, data subjects ask for more safeguards, but often give their information away without considering the potential consequences and risks. On the other hand, developers consider data protection as a value, but have no tools which allow them to make this value part of their approach in developing new solutions. Moreover, when confronted with practical issues, technology developers do not seem to be able to give this value a stable consistency. Therefore, the importance of data protection and privacy-related values is diminished and reduced to a mere question of regulatory compliance in order to avoid sanctions.

When the values in question are actually affirmed by developers or taken into account by users, their context-based nature poses further operational questions in terms of finding a process to embed this local and relative dimension into the assessment process. Co-design may be a solution, but there is a lack of specific guidance and tools in co-designing privacy, especially of ethically and socially oriented tools.

Finally, it is interesting to note that with regard to safety and security, IoT developers seem to be more aware of these issues. This may be the consequence of the existing regulatory framework, which is stronger in certain sectors (health, automotive or industrial) and imposes the adoption of certain procedures. It may also suggest that if there is already in place an approach (regulatory or non-regulatory) focused on operational elements, such practical guidance facilitates and encourages developers and users' perceptions of values and the consequent adoption of value-oriented solutions.

On the basis of these findings, it seems that the regulatory mix developed in Europe since 1995 with regard to data protection is only theoretically able to take into account the social and legal implications of data uses. Values are often implicitly taken into account by the different components of the regularity mix, but there is a lack of tools which can make values explicit and operationalise them.

Given the scenario described in the prior sections and the three initial research questions, the first part of the legal analysis confirms the importance of a value-oriented approach, but points out how the framework outlined by the Directive 95/46/EC has only partially provided adequate answerers in terms of operational tools. This does not mean that the regulatory mix ignores the importance of ethical and social values, but implies that it has difficulties putting them into practice in a clear and direct manner.

On the basis of these findings, the second part of the legal analysis (deliverable D4.1) will investigate whether the recently adopted GDPR is able to overcome these limits and offer new or stronger legal solutions (such as data protection risk assessment, accountability of data processors and empowerment of data subjects) to adequately give an answer to the exiting criticisms, or if different specific tools (such as PESIA) are required. In this regard, the results of this second part of the ongoing investigation seem to confirm the need for and importance of the adoption of the PESIA procedure.

At the same time, PESIA cannot be a mere empty box, reduced to the status of a procedural tool to be filled with values at the discretion of developers: it requires instead prior identification of the privacy, ethical and social values which are to be operationalised via PESIA. For this reason, from a legal perspective, the answer provided by the regulatory mix and the evolution of the regulatory scenario is both a preliminary condition and an instrument to find part of these values. Therefore, while the present deliverable and the next one (D4.1) mainly aim to investigate in which manner the legal framework could or could not foster social and ethical values, the second year of the project will mainly focus on sorting out the values which should underpin the PESIA model, which will involve extracting them from the last 20 years of experience of data protection regulation

5.0 Regulation and Standards

5.1 Introduction

This section provides a short overview of the regulation and standards affecting IoT aspects other than data protection in the EU.

In the previous section we looked at data ethics and wider social issues and how these relate to regulation in the context of data protection. Here we extend this analysis of the regulatory framework to other areas that will likely affect IoT developers while raising additional ethical considerations beyond data. For example, our survey of IoT manifestos showed extensive concerns about environmental sustainability, which is partly regulated in Europe through various directives on hazardous materials and electrical waste. Attitudes from developers here could range from basic compliance with the law to best practice sustainable sourcing of materials.

Although currently there is little IoT specific regulation, IoT is affected by many existing laws and subjected to a bewildering panoply of standards and frameworks. Despite the lack of direct IoT regulation - on both sides of the Atlantic as we discuss below - there are myriad issues and conflicts in the sector that require intervention, and it is unclear how long policy makers will refrain from legislating. Balancing regulation with an environment where free innovation can flourish is a slow and difficult process.

Privacy, security, and consumer trust appear to be key concerns, but 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, but it is difficult to see how top down intervention could fix these challenges without inhibiting innovation.

In the following sections we also look at standards in more detail. Technical standards are a critical aspect of the modern world, and any emerging area such as IoT will go through a convoluted process of standard setting that it is expected will eventually lead to broad interoperability of systems. It is worth reminding ourselves that there is no hard law setting that this has to always be the case though.

Standards are important for developers for practical reasons. In many cases, working under a particular technology will be the single most important decision a developer may make. This will have implications for who can use her 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 ethical considerations.

This research is part of the VIRT-EU Task 2.4 *Research on policies and institutional contexts for data identification, collection and analysis in Europe*.

It is also expected that this document may serve as a useful map for IoT designers to understand compliance issues and/or the various standards and guidance available.

5.2 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.[171] 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.

5.2.1 Unit e4 of the European Commission

The European Commission's Unit e4[172] 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.

5.2.2 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)[173]. 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".[174]

---

[171] 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

[172] 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

[173] 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/

[174] 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

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.

5.3 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.[175] 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.[176]

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.[177]

[175] Standardisation requests - mandates - Growth - European Commission. (n.d.) Retrieved November 27, 2017, from https://ec.europa.eu/growth/single-market/european-standards/requests_en
[176] 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
[177] CENELEC - About CENELEC - Who we are - European partners. (n.d.). Retrieved November 27, 2017, from https://www.cenelec.eu/aboutcenelec/whoweare/europeanstandardsorganizations/

The ANEC[178] 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.[179] 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.[180]

5.4 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.[181] 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."[182]

The US Senate has introduced the Developing Innovation and Growing the Internet of Things Act or the DIGIT Act,[183] 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.

---

[178] 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

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

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

[181] 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

[182] 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/

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

The Federal Communications Commission is opening spectrum[184] 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.[185]

5.5 China

China is a key player in digital technology and IoT in particular.[186] 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[187].

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[188]. 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.[189] 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.[190]

---

[184] 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

[185] 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

[186] 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

[187] 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/

[188] 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

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

[190] 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

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

5.6 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.[191]

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.[192] 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

[191] 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/

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

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[193] - 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.

5.7 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.

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

The Open Systems Interconnection[194] (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[195]. 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[196] (MQTT) and the web-based Constrained Application Protocol (CoAP)[197].
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.

[194] 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
[195] Russell, A. L. (2014). Open Standards and the Digital Age. Cambridge University Press.
[196] OASIS. (2014). MQTT Version 3.1.1
. Retrieved November 27, 2017, from http://mqtt.org/
[197] Bormann, C. (n.d.). CoAP — Constrained Application Protocol | Overview. Retrieved November 27, 2017, from http://coap.technology/

- 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.[198]

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[199].

5.8 Global Standards Bodies

The Internet of Things involves telecommunications and electronics technologies that are generally standardised at the international level by a handful of institutions. As

[198] 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

[199] 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/

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.

5.8.1 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)."[200]

Since then, work at the ITU has moved to *ITU-T Study Group 20 - Internet of Things, smart cities and communities*,[201] 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*[202] - that provides specifications for various layers including the lowest levels, and was originally developed for the Z-Wave technology discussed below.[203]

5.8.2 ISO/IEC

[200] 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

[201] 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

[202] 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

[203] 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

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[204] - mainly around sensor networks - under its technical committee "JTC 1 Information technology" and a draft Reference Architecture[205] 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.[206] 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.[207]

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*.[208] The specification has been developed in conjunction with the Hypercat Alliance[209], 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.

5.8.3 Institute of Electrical and Electronics Engineers (IEEE)

[204] 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

[205] 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

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

[207] 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*.

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

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

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".[210]

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.[211]
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.[212]

5.8.4 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."[213] 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

[210] IEEE. (n.d.). IEEE About IEEE. Retrieved November 27, 2017, from https://www.ieee.org/about/about_index.html
[211] IEEE. (2015). *IEEE SA - 2413 - Standard for an Architectural Framework for the Internet of Things (IoT)*. *standards.ieee.org*.
[212] IEEE. (n.d.). Internet of Things Related Standards in Development. Retrieved November 27, 2017, from http://standards.ieee.org/innovate/iot/projects.html
[213] IETF. (n.d.). About the IETF. Retrieved November 27, 2017, from https://www.ietf.org/about/

several working groups developing standards related to IoT[214] 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.[215]

The IETF also maintains the Constrained Application Protocol[216] (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.[217] 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.

5.8.5 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[218], originally designed by IBM for satellite communications with oil-field equipment.[219] This standard has now been approved by ISO/IEC as well.[220]

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

---

[214] Keränen, A., & Bormann, C. (2016). Internet of Things: Standards and Guidance from the IETF. *IETF Journal*.
[215] Zigbee Alliance. (n.d.). Zigbee IP and 920IP. Retrieved November 27, 2017, from http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeeip/
[216] Shelby, Z., Hartke, K., & Bormann, C. (2014). *IETF RFC 7252: The Constrained Application Protocol (CoAP)*.
[217] 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
[218] OASIS. (2014). *MQTT Version 3.1.1*
. *mqtt.org*.
[219] Piper, A. (n.d.). *IBM Podcast*. Retrieved from https://www.ibm.com/podcasts/software/websphere/connectivity/piper_diaz_nipper_mq_tt_11182011.pdf
[220] OASIS. (n.d.). OASIS MQTT Internet of Things Standard Now Approved by ISO/IEC JTC1 | OASIS. *oasis-open.org*.

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[221] - that has recently published its first drafts. The consortium's stated objective is to reduce fragmentation through royalty-free platform independent standards.[222]

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.

5.8.6 GSMA / 3GPP

Modern mobile telephony industry standards are mainly hosted by the 3rd Generation Partnership Project (3GPP)[223]. 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[224], or specifications.[225] The association also has important role in the development of the embedded SIM cards that allow quick remote change of providers or roaming[226]. 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

[221] W3C. (n.d.). W3C Web of Things Working Group. Retrieved November 27, 2017, from https://www.w3.org/WoT/WG/
[222] W3C Begins Standards Work on Web of Things to Reduce IoT Fragmentation | W3C News. (2017, February 24). *w3.org*.
[223] 3GPP. (n.d.). 3GPP. Retrieved November 27, 2017, from http://www.3gpp.org/
[224] 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/
[225] GSMA. (n.d.). GSMA Documents. Retrieved November 27, 2017, from https://www.gsma.com/newsroom/gsmadocuments/
[226] GSMA. (2013). *Embedded SIM Remote Provisioning Architecture Version 1.1*

the spectrum as opposed to newer low power long range technologies that can use freely available spectrum.[227] 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.

5.9 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.[228]

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.

5.9.1 OneM2M

[227] 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/
[228] Wi-Fi Alliance. (n.d.). Wi-Fi HaLow. Retrieved November 27, 2017, from https://www.wi-fi.org/discover-wi-fi/wi-fi-halow

The OneM2M group[229] 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.[230]

Their work includes a suite of standards for machine-to-machine and other IoT applications, including a set of security solutions.[231]

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.

5.9.2 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[232] 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"[233] that allows devices to work together.

---

[229] 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

[230] 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

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

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

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

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[234] 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).[235] 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.

5.9.3 IPSO Alliance

The IPSO Alliance[236] 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.

---

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

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

[236] 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

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 Things*, and the use of web technologies.[237] IPSO has worked with the standards bodies discussed in the previous sections and also with the Zigbee project,[238] which has since expanded their technology to IPv6.

5.9.4 Open Mobile Alliance

The Open Mobile Alliance (OMA)[239] 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[240], 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.

5.9.5 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,

---

[237] 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
[238] Wikipedia. (n.d.). IPSO Alliance - Wikipedia. Retrieved November 27, 2017, from https://en.wikipedia.org/wiki/IPSO_Alliance
[239] Open Mobile Alliance. (n.d.). Open Mobile Alliance Mobile Phone Standards & Specifications. Retrieved November 27, 2017, from http://openmobilealliance.org/
[240] Open Mobile Alliance, open. (n.d.). Lightweight M2M (LwM2M). Retrieved November 27, 2017, from http://openmobilealliance.org/iot/lightweight-m2m-lwm2m

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.[241]

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.[242] There is growing standardisation in this sector[243] although closed proprietary systems are still popular. Below we give an overview of some of the main initiatives.

5.9.6 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,[244] 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.[245]

5.9.7 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.[246] The

[241] 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/

[242] 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/

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

[244] 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

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

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

alliance provides a certification programme for its members[247]. The technology is based on closed intellectual property, but it is available for implementation.

Lorawan is the main technology supported by The Things Network,[248] 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.

5.9.8 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[249] 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.

5.9.9 Cellular Standards

3GPP has developed a set of standards for IOT, which include includes NB-IOT, eMTC and EC-GSM-IoT.[250]

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.

---

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

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

[249] 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

[250] 3GPP. (2016, June 22). Standardization of NB-IOT completed. *3gpp.org*.

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 Home Automation

Another 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.

5.10.1 Thread

Thread[251] 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.[252]

5.10.2 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.[253] This is incompatible with the

[251] Thread Group. (n.d.). Home. Retrieved November 27, 2017, from https://threadgroup.org/
[252] Openthread. (n.d.). Openthread. Retrieved November 28, 2017, from https://github.com/openthread/openthread
[253] 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/

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.[254]

The alliance has also developed Zigbee IP,[255] as an open internet compatible protocol based on IETF's 6LoWPAN and other specific technologies.[256]

The consortium is also developing an application layer protocol called Dotdot[257] to simplify interoperability for developers.

5.10.3 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[258], and the device specifications have been made available, including as the ITU[259] standard. Manufacturers that want to build commercial Z-wave devices must go through the alliance's certification process however.

5.10.4 Bluetooth

The new Bluetooth Low-Energy (BLE)[260] – 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

---

[254] 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/

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

[256] 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

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

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

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

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

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.

5.11 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.

5.11.1 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'[261] 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'[262] covers authorisations for all electronic communications networks and services, whether they are provided to

[261] 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')

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'[263] 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'[264] 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'[265] 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).[266]
- Regulation (EU) No 531/2012 on roaming on public mobile communications networks[267] 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

[262] 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)
[263] 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)
[264] 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)
[265] 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).
[266] 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
[267] 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)

undermined the investment incentives of both new entrants and incumbent operators".[268]

They promote instead the concept of "infrastructure competition"[269] 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.

5.11.2 The European Electronic Communications Code

In September 2016, as part of the new "Connectivity Package"[270] the European Commission published its proposal for a directive establishing the European Electronic Communications Code.[271] 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.

---

[268] 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

[269] 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

[270] 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

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

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."[272]

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."[273]

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.

5.11.3 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[274] (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

[272] as above.

[273] 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/

[274] 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)

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.[275]

5.12 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.[276] 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 l*aying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications*

[275] 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

[276] 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/

networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.[277]

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.[278] The European regulatory body BEREC provides guidelines for implementation.[279]

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.[280] 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.

5.13 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".[281]

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

[277] 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

[278] 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

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

[280] 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/

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

actor on the supply chain, from designers and suppliers to importers and distributors when the product is made available in the EU.[282]

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.[283]

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.

5.14 The Blue Guide

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

[283] 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

The 2016 'Blue Guide'[284] 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.

5.14.1 Product Directives

Radio Equipment Directive

The Radio Equipment Directive 2014/53/EU[285] (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.[286]

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

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

[285] 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

[286] 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*

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.[287]
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.[288]

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".[289]

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.

5.14.2 Radio Spectrum Decision

In addition to the RED, another element of radio regulation is the Radio Spectrum Decision (676/2002/EC).[290] 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

[287] 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

[288] 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

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

[290] 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)

developers will probably only need to have a simple understanding. We briefly discuss some of the relevant spectrum issues below.

5.14.3 Low Voltage Directive

The Low Voltage Directive 2014/35/EU (LVD[291]) 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.

5.14.4 Electromagnetic Compatibility Directive

The Electromagnetic Compatibility Directive 2014/30/EU (EMCD)[292] 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.[293] 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.[294]

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

[291] 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)
[292] 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)
[293] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety
[294] 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

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.[295]

5.15 Toy Safety

In Europe, toys fall within the scope of multiple standards and directives.[296] Electronic and radio enabled toys will have to comply with technical regulations described in the previous section.[297] 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[298], 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.[299]

5.15.1 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".[300] It is possible that the actual number will be lower, and that

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

[296] 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

[297] 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

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

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

[300] 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

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.[301] The regulations are incredibly complex. Particularly relevant for IoT developers is the Motor vehicles (Regulation (EC) 661/2009)[302], 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[303]. 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[304], ensuring that nobody is left without insurance cover in the event of an accident.

5.16 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[305] 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.[306]

5.16.1 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

[301] 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

[302] 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

[303] 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

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

[305] 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/

[306] 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

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[307] 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.[308]

5.17 Further Reading:

- The Low Power Radio Association is a source of information and potential support for IoT developers.[309]
- Comprehensive information on the regulatory environment is provided by ETSI and CEPT/ECC.[310]
- A case study illustrating how regulations and standards come together in practice is provided by the RFID in Europe association.[311]

5.17.1 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".[312]

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

[307] European Communications Office. (n.d.). ECO Documentation v5.1. Retrieved November 28, 2017, from http://www.ecodocdb.dk/
[308] CEPT. (2017). *ERC Recommendation 70-03 Relating to the use of Short Range Devices (SRD)*. *erodocdb.dk*.
[309] LPRA. (n.d.). Low Power Radio Association. Retrieved November 28, 2017, from http://lpra.org/
[310] ETSI, CEPT/ECC. (2016). *The European regulatory environment for radio equipment and spectrum: an introduction*. *etsi.org*.
[311] Standards & Regulations | RFID in Europe. (n.d.). Retrieved November 28, 2017, from http://www.rfidineurope.eu/sr
[312] CEPT. (n.d.). About CEPT. Retrieved November 28, 2017, from https://cept.org/cept/

key space for information, harmonisation, and management of radio spectrum use[313] 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),[314] 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).[315]

5.17.2 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.[316]

---

[313] CEPT. (n.d.). ECC. Retrieved November 28, 2017, from https://cept.org/ecc/
[314] CEPT. (n.d.). ECC and ETSI. Retrieved November 28, 2017, from https://cept.org/ecc/ecc-and-etsi
[315] 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/
[316] ETSI. (n.d.). Work Item Plan: All Active Work Items For Directive '2014/53/EU'. Retrieved November 28, 2017, from http://bit.ly/2u1oiy2

In addition to RED and the multitude of other telecoms standards, ETSI has many standards specifically relevant to IoT development[317], 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.[318]

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).

5.17.3 CEN/CENELEC

The European Committee for Standardisation[319] (CEN) and the European Committee for Electrotechnical Standardisation[320] (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[321], including the regulation of plugs and sockets.[322]

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[323].

5.18 Telecoms Issues in IoT

[317] ETSI. (n.d.). Internet of Things.
[318] ETSI. (n.d.). *TR 103 376 - V1.1.1 - SmartM2M; IoT LSP use cases and standards gaps*. *etsi.org*.
[319] CEN. (n.d.). Who we are. Retrieved November 28, 2017, from https://www.cen.eu/about/Pages/default.aspx
[320] CENELEC. (n.d.). CENELEC - About CENELEC - Who we are. Retrieved November 28, 2017, from https://www.cenelec.eu/aboutcenelec/whoweare/
[321] CENELEC. (n.d.). Household appliances. Retrieved November 28, 2017, from https://www.cenelec.eu/aboutcenelec/whatwedo/technologysectors/householdappliances.html
[322] 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
[323]European Commission Standardisation mandate in the field of information and communication technologies applied to radio frequency identification (rfid) and systems M 346 2008

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.[324] 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.[325]
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[326]. 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.

5.18.1 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.

---

[324] BEREC. (2016). *BEREC Report on Enabling the Internet of Things*. *berec.europa.eu*.
[325] Brown, I. (2015). *GSR discussion paper: Regulation and the Internet of Things*. *itu.int*.
[326] 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

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.[327]
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,[328] 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.[329]

5.18.2 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,[330] 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[331], 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

[327] GSMA. (2013). *Embedded SIM Remote Provisioning Architecture Version 1.1*
[328] 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/
[329] BEREC. (2016). *BEREC Report on Enabling the Internet of Things*. *berec.europa.eu*. (p. 32)
[330] ibid.
[331] EY. (2015). Enabling the IoT environment. *EY Inside Telecommunications*, (17).

says that each case needs to be considered on its own terms. Regulators and industry have asked for more clarification on this issue.[332]

5.18.3 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.*[333]

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.

5.18.4 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.

[332] 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/

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

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.[334]"

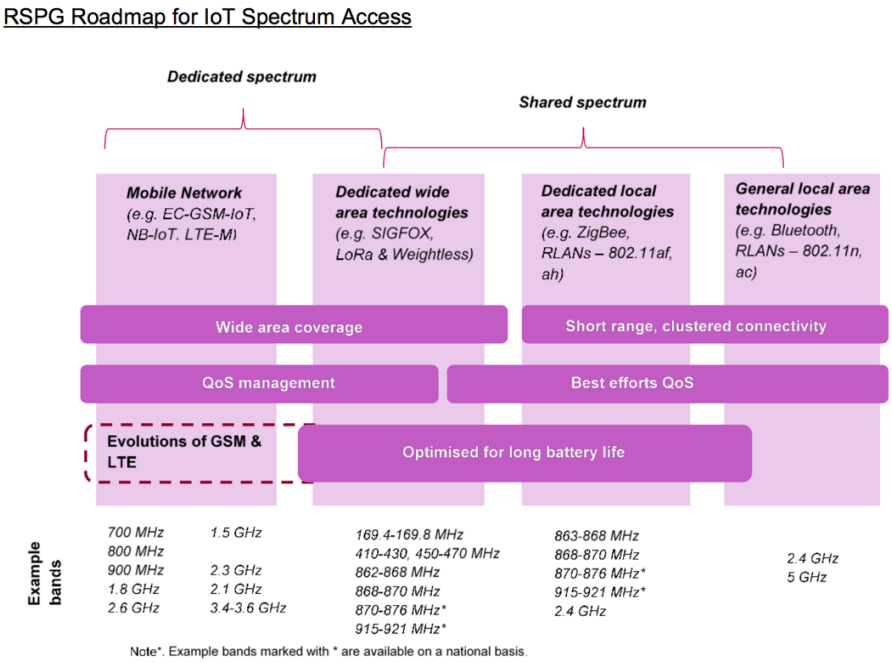

Figure 6[335]

5.19 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.

5.19.1 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.[336] Cybersecurity is

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

seen as one of the main challenges, despite assurances from the electrical industry[337]. 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.

5.19.2 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.[338]

Common issues include under or over voltage, transient spikes and complex distortions of electrical signals that can damage components and also cause humming noise[339] 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.[340] Energy efficiency is another important aspect[341], 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.

5.19.3 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[342].

---

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

[337] 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/

[338] 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/

[339] 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/

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

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

[342] Chitravanshi, R. (2016, December 29). Apple seeks relaxed labelling rules, doesn't want to print product info on devices. Retrieved November 28, 2017, from

Some IOT devices may require even further information and weather resistant rip-proof labels.[343] 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[344] that allows for information to be displayed electronically[345]. The EU maintains strong labelling requirements, the most important of which is the CE marking.

5.19.4 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*.[346]

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.[347]

5.20 Consumer Protection

Consumer organisations, such as Consumers International, have raised concerns about the Internet of Things[348]. 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

---

https://economictimes.indiatimes.com/tech/hardware/apple-seeks-relaxed-labelling-rules-doesnt-want-to-print-product-info-on-devices/articleshow/56229190.cms

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

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

[345] 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

[346] 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

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

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

products that include hardware and software, which can be remotely controlled, and where it is unclear whether the notion of ownership applies anymore.[349] These issues if unchecked will lead to vendor lock-in through lack of interoperability and a lack of choice.

Other discussions[350] 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.[351] 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)[352] 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.[353] 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.

5.20.1 Liability

The legal basis of product liability law in Europe is Product Liability Directive 85/374/EC[354] (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.

---

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

[350] 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/

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

[352] 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

[353] 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

[354] 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

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.[355] Liability for self-driving cars is already being worked out at the national level in various countries.

5.21 Social

5.21.1 Environmental

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)[356]

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.

[355] 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

[356] 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

Restriction of Hazardous Substances in Electronic Equipment Directive 2011/65/EU (RoHS 2)[357]

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)[358]

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.[359]

Environmental regulations on electronics seem to have delivered some positive results[360], 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.[361] Greenpeace looks at the sustainability of the design, including the ease of repairs and part replacement.

5.22 Labour

[357] 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.

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

[359] 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

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

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

A 2012 report found that the electronics sector had the worst labour conditions of any industry[362]. 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.[363]

The Clean Electronics Production Network (CEPN) was launched in 2016 to reduce exposure to hazardous materials by workers in the electronics supply chain.[364] The development of ethical supply chains is advancing slowly, led among others by Dutch NGO and phone manufacturer Fairphone.[365]

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

5.23 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

[362] 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/

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

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

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

creative works. Directive 2009/24/EC on the Legal Protection of Computer Programs[366] 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.

5.23.1 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.*[367]

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.

5.23.2 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.

---

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

[367] 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

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.[368]

5.23.3 Database Directive[369]

Data ownership, access and control are central issues in IoT. Databases can be protected under the EU *sui-generis* database right.[370] 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.

5.23.4 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*[371]. 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",[372] 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.

---

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

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

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

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

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

5.23.5 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.[373]

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.

5.23.6 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,[374] 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

[373] 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

[374] 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

exceptions where it is lawful to break DRM, such as “ripping” DVDs[375]. 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.

5.23.7 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

[375] 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

new directive that would promote the free flow of non-personal data by removing localisation requirements and cross-border obstacles.[376]

5.24 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[377] 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[378] and Cisco[379]

[376] 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

[377] 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

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

are publishing their own security policies and frameworks for IoT. Below is a summary of frameworks that may be more relevant to developers.

5.25 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.

5.25.1 The NIS Directive

The Directive on security of network and information systems (the NIS Directive)[380] 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.

---

[379] 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

[380] 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

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[381].

5.25.2 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.[382] 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.[383]

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.[384]

5.26 Frameworks and Guidance

5.26.1 IoT Security Foundation

The IoT Security Foundation (IoTSF)[385] 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

[381] 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/

[382] 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")

[383] 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

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

[385] 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

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[386] 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.

5.26.2 Cloud Security Alliance

The Cloud Security Alliance[387] 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.[388]

5.26.3 OWASP

The Open Web Application Security Project (OWASP)[389] 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[390] 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.

5.26.4 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

---

[386] ibid.
[387] Cloud Security Alliance. (n.d.). Home - Cloud Security Alliance. Retrieved November 28, 2017, from https://cloudsecurityalliance.org/
[388] Cloud Security Alliance. (2016). *Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products*. *downloads.cloudsecurityalliance.org*.
[389] 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
[390] OWASP. (n.d.). IoT Security Guidance. Retrieved November 28, 2017, from https://www.owasp.org/index.php/IoT_Security_Guidance

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[391] 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.

5.26.5 Online Trust Alliance

The Online Trust Alliance (OTA)[392] is an initiative within the Internet Society (ISOC),[393] 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[394] 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.

5.26.6 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[395] works on Industrial Automation and Control Systems Security, and currently includes over 500 international industrial cyber security experts. This work

---

[391] Broadband Internet Technical Advisory Group. (2016). *BITAG Report - Internet of Things (IoT) Security and Privacy Recommendations*. *bitag.org*.
[392] Online Trust Alliance. (n.d.). Online Trust Alliance. Retrieved November 28, 2017, from https://otalliance.org/
[393] Internet Society. (n.d.). Home | Internet Society. Retrieved November 28, 2017, from https://www.internetsociety.org/
[394] Online Trust Alliance. (2017). IoT Security & Privacy Trust Framework v2.5. otalliance.org.
[395] 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

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[396] 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.

5.26.7 Industrial Internet Consortium

The IIC as discussed above is managed by the OMG, which as discussed provides frameworks, not standards. Their framework for security[397] contains useful information for developers thinking about security but implementing its systematically is certainly overkill for independent designers.

5.26.8 GSMA

The GSMA security guidelines for IoT[398] 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.

5.27 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.

The development of the PESIA framework will need to consider some of these broader issues, particularly from a virtue ethics approach, which lends itself to a more holistic perspective, rather than isolated outcomes.

---

[396] 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

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

[398] GSMA. (2016). *IoT Security Guidelines Overview Document Version 1.0*. *gsma.com*.

6.0 Formulation of Domain Requirements: Processes for integrating Network, Policy and Qualitative Research

Our process for integrating research is based on work across interdisciplinary teams and synthesis workshops, where the entire consortium presents findings as well as works together through coordination by CIID to synthesize new questions and interdisciplinary approaches (Task 2.6). We also undertook a data sprint on Wednesday, November 8, 2017 led by consortium member Rachel Douglas-Jones, who leads the ITU ETHOS lab (Task 2.6).

6.1 Synthesis Workshop

Our VIRT-EU consortium synthesis workshop was held on October 28, 2017. In order to define how we would move forward and respond to the advisory board's inputs, we each wrote down three key questions we hoped to address:

- How do we use pathological cases to surface people's expectations about how IOT works?
- How can we do this across disciplines?
- How can we describe resistant developer communities? Absence, challenge, failure?
- When do ethical discussions happen and how do we investigate this?
- Is the goal of our work to improve processes and practices or to create conversation?
- How do we address the problem of emergent ethical problems?
- How might we manage macro/micro contexts (ie. examine policy to see how developers resist larger systems)
- What papers are we planning to write?
- How can we evaluate the impact of our work?
- Are quality and impact related?
- How can the PESIA model facilitate how IoT developers *do* ethical thinking?
- Why should IoT developers be interested in adopting PESIA?
- Can we collect and visualise anxieties about IOT from the different groups we meet (visualizing contrasting anxieties)?
- In what creative ways can we make the closed-ness of open things visible? (ie. standards setting)
- How do we conceptualise and materialise intervention in this large and divergent space?
- How can we think about IoT and ethics as occasions?

- Can we collectively exemplify how we might represent ethics, working with a sense of ethics as contextual and relational?
- If our preconceptions about when/where IoT discussion spaces occur were incorrect, what process should we use instead to choose physical sites?
- How can we use Meetup data if conversation happens face to face?
- What are the boundaries of our project in terms of industries and ethical approaches?
- What is IoT?
- How do we take into account the system/level/stack that the people we work with are dealing with?
- Who should be in our workshops?
- How we can use 'artificial cases/horrible cases' as study points for all of us? Do those cases have to be the same across the project?
- What are the attributes of a good field site?

We clustered the long list of questions into the following topics:

1. How do we integrate PESIA into the rest of the project's work?
2. What is the potential role of pathological cases in our project? How do we collaboratively define the stories / cases that should be considered by the different partners in the project?
3. Where should the field sites be for the upcoming phases of field research and workshops? What are the attributes that define a suitable field site for VIRT-EU?

We broke into small, interdisciplinary groups to consolidate our understandings and try to find possible ways to address emergent issues. We then presented our summaries to the larger group, and, in response, CIID created various diagrams that all the partners could edit, question, and approve. These diagrams served as mechanisms for making the general discussion and debate more visible - as we could all see the edits reflecting any given contribution or critique.

6.2 PESIA

The timing and integration of PESIA was one of the key topics of clarification. The small group took on the PESIA question and presented the following plan, upon which all partners agreed: that the legal team plans to create a first draft of the PESIA model by M24, that they will then give to the ethnographic and co-design teams to test with developers. During the initial drafting, the legal team will be open to suggestions and inputs from the ethnography team based on their field research thus far. And - after the first draft is ready - the incorporation into the developer workshops and ethnography interviews will allow for quick feedback to the legal team before creating a final version. We also discussed the critical question of why PESIA could be useful to developers - why they would want to use it at all. We considered this issue and came up with the following possible streams of adoption paths:

1. Many of the developers / companies we will be studying and working with will not have enough money to hire an ethicist in-house, however, they would like to have a clear assessment they can consider their work in relation to so that they can reduce their own sense of uncertainty and fear in relation to potentially crossing legal and ethical lines.
2. In terms of an "authority" that might compel uptake, the two possibilities here are a formal regulatory authority and a more bottom-up approach of a critical mass who might promote the use of PESIA through their social networks and various communication platforms.

6.3 Pathological Cases

A second team considered the role of pathological cases - given the potential noted by our advisory board as well as our own consortium - how might we integrate and methodologically consider pathological cases as part of our research and development?

What we need to identify: pathological cases that show glaring ethical issues according to the courts - cases that specifically focus on locations, industries and company sizes that are also corresponding to the field sites and companies we seek to study.

The small team considering this question about pathological cases focused on two aspects: 1) Why use pathological cases at all? 2) How do we identify these cases? We were aware that each partner in the project can use the cases in different ways. However, we agreed that POLITO/ORG will be responsible for identifying several potential cases based on how they are being discussed in the courts. The fieldwork teams will test their use and relevance in the field and give feedback to POLITO/ORG.

The use cases that each might have are - for POLITO/ORG, using the cases in the discussion of certain ethical issues during the prototype survey or questionnaire they plan to create to fuel certain unanswered aspects of their PESIA questionnaire. For the fieldwork teams of ITU and LSE, the pathological cases may be used during qualitative interviews. Lastly, for the online analysis of UU, the pathological cases may be considered as a way to identify crucial conversations and meaningful actors - as well as how their inputs impact the flow of a given conversation.

6.4 Fieldwork Site Identification

Lastly, a third small team presented the attributes we collaboratively decided upon and defined for fieldwork site identification - based on input from the advisory board overall, as well as our fieldwork thus far. These are attributes that the VIRT-EU team hopes will allow enough focus to understand the complicated issues around IOT deeply enough and to conduct meaningful workshops for the IOT developers and our own team. The following attributes will define a field site for VIRT-EU.

1. That the qualitative team has evidence from their fieldwork that indicates location likely to have a dense and connected network of developers
2. That the quantitative team has supporting similar evidence from Meet-up

    a. Attendance should be above a certain threshold
    b. Frequency of meet-ups should be more than a (given) number of times per month or year
    c. Topics of meet-up should be diverse (though IoT-focused)
3. To note:
    a. What type of regulation is present in regards to IoT? Hard, soft, or none at all?
    b. What is the type of development occurring primarily? Hardware or software or mixed?
    c. What is the company size?
4. Bonus attributes of a field site location would be:
    a. Advisory board recommends site and shares contacts of developers / companies
    b. Literature identifies the site as having many of the features of 1, 2

6.5 Data Taxonomies Linking Fields

As the quantitative team at Uppsala University is considering how to integrate their work with the qualitative team's work, the idea of a "taxonomy" has been introduced over the past few months. In relation to this, Uppsala led a discussion of the potential of a taxonomy and CIID supported this discussion with a theoretical mapping tool.
We divided our consortium into small groups and gave them cards to define the community and values that could be tagged to a given network of individuals who might be automatically gathered and parsed by the quantitative system that can identify this network of individuals solely based on a hashtag. However, this visual network requires more descriptive analysis - and the quantitative team hopes to involve the ethnography team in this exercise.

> "If I knew who the individuals were in the network, it would be useful because we could say this group of people we know ignore all of these things we put around the edges. The problems of interoperability and security are not discussed at the conferences they go to. Then we can elicit the knowledge we have about these people and discuss this with them."

> "Given these terms - people interested in sustainability - they will probably discuss transparency, responsibility, but they may not discuss security."

> "We did almost the same except we had a hypothesis related to the qualities related to that strong cluster. Let's say - we are at an industry-IOT conference. Security will be a top value, interoperability is the second. Because this is about sectors, compliance, the values of education and sustainability are not considered… but if we had gone to Mozfest, we would have a very different set of values in the middle, and this can be explained by culture that is underlying all of this."

6.6 Network and Qualitative Integration: Data Sprint

In addition to the full consortium synthesis workshop, we also held two smaller synthesis workshops to bring together our qualitative and network research teams: one on August 26th in Uppsala and one on Nov 8th 2017 in Copenhagen, structured as a data sprint. At the August 26th 2017 project meeting, we agreed that it would be beneficial for the qualitative and quantitative scholars to convene around the twitter datasets being collected on Twapperkeeper (Task 2.6). ITU VIRT-EU member Rachel Douglas-Jones proposed a day-long "Data Sprint" to familiarise the qualitative researchers with the data that had been collected through Twapperkeeper so far, to explore what kinds of questions could be asked of this data, and to test out the new functions being developed by the Uppsala team on the analysis platform.

A data sprint is a growing form of analysis that originates in the Digital Methods Initiative, based at the University of Amsterdam[399]. Its precise methods vary according to which research group is coordinating the exercise, but they are most simply described as intensive research workshops, 'where participants coming from different academic and non-academic backgrounds convene physically to work together on a set of data and research questions[400]. They are also a community building exercise, whether that community is based within a student group or public participants[401]. During 2016, the ETHOSLab hosted or co-organised 15 data sprints and its approach is rooted in taking the exploration of quantitatively collected data through and with qualitative scholars (Laursen 2016), although a variety of formats exist within the Copenhagen area. Given the methods affordances, we deemed the data sprint an excellent way of addressing Task 2.6 Synthesis of findings and formulation of domain requirements, as it brought together research group members involved in the domain exploration of 2.2. around the data collected under Task 2.1.

In her role as co-head of ITU's ETHOSLab, Rachel Douglas-Jones worked with the Lab Manager and Lab Assistant Marie Blønd and Cæcilie Sloth Laursen (respectively) to prepare a day of activity where the qualitative and quantitative scholars could meet and discuss around IoT related twitter datasets collected by the Uppsala VIRTEU team through Twapperkeeper. As Venturini et al. note, Data sprints are 'always preceded by a long and intense work of preparation' (p. 2) since most of the research infrastructure should be in place once participants convene. The project's active ethnographers Ester Fritsch (ITU) and Selena Nemorin (LSE) were approached for hashtags they had registered on Twapperkeeper that they were particularly curious to explore. Once these had been identified, on October 8, 2017 the ITU team entered into dialogue with the Uppsala team to begin the preparations for the event. The ITU team required downloaded datasets with a particular file configuration, which would work with software

[399] Venturini, T., Munk, A. K., & Meunier, A. (2016). "Data-sprint: A public approach to digital research" in *Interdisciplinary Research Methods* C. Lury, P. Clough, M. Michael, R. Fensham. S. Lammes, A. Last and E. Uprichard, Eds. (Forthcoming)

[400] Munk, A. K.. Meunier, A. & Venturini, T. (2017). Data Sprints: A Collaborative Format in Digital Controversy Mapping. *Digital STS Handbook* New Haven, CT: Princeton University Press.

[401] Laursen, C. S. (2016). The promise and premise of data sprints: an inquiry of data sprints as an emerging method. (16 December, 2016), *Innovation and Technology in Society*. See https://ethos.itu.dk/2017/02/15/caecilie-laursen/

programs Tableau and Gephi, which required the addition of a separate hashtag column for the production of cohashtag graphs.

Data-sets

#LTW (31,000 tweets), #iotmark (446 tweets), #iotweek (2500 tweets). London merged datasets (46000 tweets) Geneva merged dataset (2750 tweets)

Davide Vega D'aurelio worked with the ITU team to generate three key single hashtag datasets for the hashtags and two combined datasets, based on events in London and in Geneva. The programs Tableau and Gephi were chosen due to the ETHOSLab team's familiarity with them. The stated objectives of the day were to:

- Familiarise ourselves with what we have collected so far;
- Familiarise ourselves with working with Twitter data, and learning what kinds of qualitative questions we can ask of it;
- Become more familiar with visualisation techniques and what they can produce; and
- Find limitations in our existing platform, to help the VIRT-EU team customise its capacities to our interests.

The outcomes of the data sprint were as follows.

1. Tableau enabled timelines for the hashtags #iotmark, #LTW, and #iotweek, allowing participants (in groups of 3-4) to closely analyse the tweets generated around a particular topic or event. The organisers considered the Tableau visualisation a basic first step in becoming familiar with the data, because the ethnographers who had participated in the events on the ground could, in this format, read the content of the tweets.
2. A set of co-hashtag and user-hashtag visualisations for each of the hashtags and the joint datasets.
3. A 12-page summary of the event where the hashtag teams presented their most intriguing or insightful visualisations, and produced commentaries on them, or questions arising. This document included a series of reflections by the qualitative team on the new kinds of questions they could ask of the twitter data, once they had seen it in use, and how their research practices might be appropriately adjusted as a result of this synthesis exercise.
4. Capacity building between the qualitative and quantitative scholars based at ITU in terms of ability to use the Uppsala developed tools. Based on this attempt at qualitative and quantitative analytic integration, the data sprint team developed a series of 12 questions for the developers, which were passed back to Uppsala by Luca Rossi once the data sprint was concluded.

Working across the qualitative and quantitative data to understand and explore the spaces in which IoT development takes place is challenging. The ITU based data sprint brought researchers physically together to explore and experiment with a selection of data so far collected. The primary objectives were familiarisation and synthesis of research approaches, with a view to producing better understanding of one another's research processes and requirements across the teams. Based on the dialogue during the event and the curious, respectful questions asked across the disciplinary backgrounds, this goal was achieved.

6.7 Strategies for Research Integration and Domain Specification: Summary

Our synthesis workshop and data sprint thus produced four key strategies for research integration:

1. Quick feedback loops for the development of PESIA;
2. A transdisciplinary, experimental approach to the use of ‘pathological cases’ as interview elements, soft law provocations and data to search using network methods;
3. A framework for employing legal and policy research and network mapping to facilitate a focus on particularly generative ethnographic field sites within and beyond the settings of London and Amsterdam.
4. Use of taxonomies and data visualisation strategies to link together network and ethnographic research and deepen the questions being posed.

7.0 Conclusion

This report has summarised extensive research on defining the domain of networked IoT communities across Europe and their ethical practices. It has outlined how ethical issues related to IoT have been presented in the past, how relationships among this community of practice may be mapped (and the limitations of some of the methods of doing so), the ways that ethical issues appear within discussions at influential sites including conferences and meetings, and the alternative spaces that IoT developers and activists build for themselves. This report also shows that law is often used as a limit-case in discussions among this community of practice, but that many hard and soft law and regulatory features impact this domain, and that existing ethical, legal, and standardisation frameworks only partially address the issues in the area.

Our interdisciplinary research strategy, grounded not only in a review of the communities of practice but also in an investigation of the alternative positions that groups attempt to take in relation to these ideas, reveals that openness, transparency, security and ubiquity may be ways of carrying ethical positions forward. We propose various strategies to synthesise and advance interdisciplinary research in this area, including linking definitions, data taxonomies, and data visualisations, and focusing on the 'pathological cases' that highlight risks, danger or concern over the IoT. In our next year of research we will further refine these tools to support deeper understanding of how developers of IoT projects grapple with ethical issues, and feed these insights into the development of a PESIA model and the creation of stakeholder workshops.

Appendix I: Manifestos

The following 28 documents constitute our corpus for analysis with short-codes marked in brackets.

[RIOT]

ThingsCon. 2017. *RIOT. The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin. http://thingscon.com/responsible-iot-report/

[Deschamps-Sonsino, RIOT]

Deschamps-Sonsino, Alexandra. 2017. The Whole Internet of Things. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 10-12.

[Krajewski, RIOT]

Krajewski, Andrea. 2017. User Centred IoT-Design. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 13-21.

[Villum, RIOT]
Villum, Christian. 2017. Designing the Digital Futures We Want. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 22-24.

[Dietrich, RIOT]
Ayala, Dietrich. 2017. Trust, Lies and Fitness Wearables. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 25-32.

[De Roeck, RIOT]
De Roeck, Dries. 2017. On IoT Design Processes. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 32-38.

[Scganetti, RIOT]
Scganetti, Gaia. 2017. The here and now of dystopian scenarios. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 39-48.

[Robbins, RIOT]
Robbins, Holly. 2017. The Path for Transparency for IoT Technologies. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 49-60.

[Smit, RIOT]
Smit, Iskander. 2017. Touch base dialogues with things: Responsible IoT & tangible interfaces. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 61-68.

[Jorge, RIOT]
Appiah, Jorge. 2017. IoT in Africa: Are we waiting to consume for sustainable development? *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 69-73.

[Krüger, RIOT]
Krüger, Max. 2017. Expanding the Boundaries for Caring. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 74-78.

[Thorne, RIOT]
Thorne, Michelle. 2017. Internet Health and IoT. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 79-82.

[Bihr, RIOT]
Bihr, Peter. 2017. We need a more transparent Internet of Things. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 83-87.

[Kranenburg, RIOT]
Van Kranenburg, Rob. 2017. How to run a country (I know where that door is). *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 88-91.

[Burbidge, RIOT]
Burbidge, Rosie. 2017. Design and branding: what rights do you own and what pitfalls should you watch out for? *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 92-97.

[Haque, RIOT]
Haque, Usman. 2017. How Might We Grow Diverse Internets of Things? Learning from Project Xanadu & the WWW. *The State of Responsible Internet of Things (IoT)*. Published by ThingsCon, Berlin, 98-102.

[Ethical Design]
Balkan, Aral. 2015. Ethical Design Manifesto. Retrieved July 6 from https://ind.ie/ethical-design/.

[Doteveryone]
Doteveryone, 2017. Exploring what "responsible technology means". Retrieved September 14, 2017 from https://medium.com/doteveryone/exploring-what-responsible-technology-means-4f2a69b50a61

[Dowse]
Dowse. Retrieved May, 2017 from http://dowse.eu

[Flaws Kit]
Flaws of the Smart City Friction Kit Version 1.3. October 2016. Designed by Design Friction. Retrieved August 8 from: http://www.flawsofthesmartcity.com

[Maker Movement Manifesto]
Hatch, Mark. 2014. The Maker Movement Manifesto. McGraw Hill Education.

[IoT Design Manifesto]
IoT Design Manifesto. 2015. Retrieved March 14, 2017 from https://www.iotmanifesto.com

[Open IoT]
Mozilla's Open IoT Studio. 2016. *Practices for a Healthy Internet of Things*. Edited by Michelle Thorne, Jon Rogers and Martin Skelly. Published by Visual Research Centre, Duncan of Jordanstone College of Art and Design, University of Dundee.

[TCM]
Oliver, Julian, Gordan Savicic and Danja Vasiliev. 2011-2017. The Critical Engineering Manifesto. Retrieved June 23 from https://criticalengineering.org

[TOPP]
Topp Studio. 2016. R.IoT. Responsible IoT. Retrieved March 30, 2017 from https://medium.com/the-conference/responsible-iot-3-essential-iot-design-features-504ce4c62e77

[Uribe]
Uribe, Félix. 2017. The classification of Internet of Things (IoT) devices Based on their impact on Living Things. Retrieved July 15 from https://www.uribe100.com/images/Documents/classificationofiotdevices.pdf

[Apps for smart cities manifesto]
The apps for smart cities manifesto. 2012. Retrieved July 6, 2017 from http://www.appsforsmartcities.com/index.html%3Fq=manifesto.html

[Human(IT)]
The Human(IT) Manifesto. 2017. Accessible manifesto from World Economic Forum 2017: BlockChain, Ethics, AI, Humans and Shift Happens. Retrieved September 11, 2017 from http://dataethicsconsulting.com/en/world-economic-forum-2017-blockchain-ethics-ai-humans-shift-happens/

[The Things Network]
The Things Network Manifesto. 2017. Retrieved July 7, 2017 from https://github.com/TheThingsNetwork/Manifest