Article

Case Study : The Internet of Things and Ethics

Antoniou, Josephina and Andreou, Andreas

Antoniou, Josephina ORCID: 0000-0003-0169-1299 and Andreou, Andreas (2019) Case Study : The Internet of Things and Ethics. The Orbit Journal, 2 (2). ISSN 2515-8562

It is advisable to refer to the publisher's version if you intend to cite from the work.
10.29297/orbit.v2i2.111

Case Study
The Internet of Things and Ethics

Antoniou, Josephina,

UCLan Cyprus, Physical Sciences and Computing, School of Sciences

Andreou, Andreas,

AEQUITAS, Cyprus

Corresponding Author: JosephinaAntoniou, JAntoniou@uclan.ac.uk

Abstract: The Internet of Things (IoT) may be defined as a network of networks, where the end devices are not user-handled devices but can be computing devices, mechanical and digital machines. In many businesses, IoT-based software is used increasingly as a means to deliver enhanced customer service and improved business management procedures. By using IoT to monitor business operations, through tracking-capable software, businesses are, for instance, able to track products and employees. The issue is further explored through literature review and a case study of a company developing IoT based monitoring software.

The review focuses on the effects of using IoT as part of Smart Information Systems, especially systems supported by 5G networks in the near future. The effects on the users of SIS are referred to by the term Quality of Experience (QoE) and the specific effects of 5G networks on QoE are discussed in this background review. Since the user experience is also affected by such actions as employee and asset monitoring with the use of IoT, a brief overview of legal aspects follows the technological details of QoE in an IoT-aware 5G system. The legal/human rights analysis is presented through the literature, and takes into account some suggestions for guidelines and policies on monitoring is offered. A dis-

cussion on ethics and perceptions around monitoring and tracking is further presented.

The CRM.COM case focuses thereafter on how the company provides tracking software as a service and as a product for businesses nationally and in several countries worldwide. The case study discusses the ethics of such IoT-powered software, by considering both their design and their usage.

Overall, the area of using IoT-based tracking and monitoring applications to assist and enhance specific business processes is growing and becoming increasingly popular, both in terms of development and use. Being a new research area, however, it lacks sufficient literature that examines the ethical, social, economic and legal implications of the use of this technology. Such studies into the design, development and use of such IoT-based applications present important relevant information that enriches the state-of-the-art literature on the topic both from an academic and a practical perspective.
This report offers an original case study on the use of an IoT related SIS in the software design and development area. Many of the ethical and legal issues discussed in this report have been analysed more generally within academia and assessed in other areas of application, but have rarely been associated with the IoT usage for tracking and monitoring. Therefore, this report will be highly valuable for the development and furthering of theory, knowledge and application for designing, developing and using such IoT based applications.

Keywords: Internet of Things, IoT, SIS, Quality of Experience, Big data, CRM.COM

Citation: Antoniou, J., & Andreou, A. (2019). Case Study : The Internet of Things and Ethics. *ORBIT Journal*, *2*(2). https://doi.org/10.29297/orbit.v2i2.111

1. Internet of Things and Ethics: A Case Study

"The Internet of Things is … the latest, most hyped concept in the IT world" (Madakam, Ramaswamy, Tripathi 2015). It is

> "An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment" (ibid.).

The Internet of Things (IoT) may be defined as a network of networks, where the end devices are not user-handled devices but can be computing devices, mechanical and digital machines. They can even be objects that can be provided with unique identifiers that transmit and receive data without active human intervention, e.g. sensors or tracking devices. This can include a person indirectly, e.g. a patient with a heart monitor; even though the person is part of the data generation process, he/she is not directly involved with the data generated and communicated over the network.

Heart monitor data, free images Benjamin Earwicker

In many businesses, IoT-based software is used increasingly as a means to deliver enhanced customer service and improved business management procedures. By using IoT to monitor business operations, through tracking-capable software, businesses are, for instance, able to track products and employees.

The use of the IoT can be associated with the generation and manipulation of vast amounts of data that may relate to human behaviour and interaction, popularly known as Big Data. Big Data and its manipulation can result in potentially high impact, for instance, on privacy, security and consumer welfare (Kshetri 2014). This is particularly so as the process of data collection in IoTis done

IoT-based software is used increasingly as a means to deliver enhanced customer service and improved business management procedures.

automatically, often without any human intervention.

IoT primarily aims at establishing machine-to-machine communications, i.e. connecting machines over a network without relying on, or requiring human intervention. The increasing use of sensor devices and the enhancement of subsequent smart environments has led to the integration of sensors within IoT, bringing the exchange of data between machines to a new level, where, contextually, data is now exchanged between environments, humans and objects through the connectivity enabled by the IoT.

This case study investigates the development and use of an IoT-based SIS that makes use of Big Data. Note that at the current stage of the SIS development, it does not use any AI-based algorithms. The ethical impact is expected to relate to the aspects of data collection and manipulation to support monitoring and tracking in businesses, where the specific SIS is used.

1.1 Business Use of IoT for Surveillance

In business, IoT proved to be a solution for saving time and money, for improving the customer experience and employee productivity, and for overall monitoring business processes. In fact, asset-tracking and monitoring are thought to be a driver for business innovation (Tournier, 2017). Following the developments in technology, according to Karahisar (2014), *monitoring* has steadily increased in several types of environments such as educational institutions, roads, subway transportations, as well as in people's habitats, (predominantly in urban settings). The same applies in the workplace. Due to the increase in *cyberloafing*[1] and consequent lawsuits, employee monitoring has become more widespread and much easier with the use of new and cheaper technologies (Mujtaba, 2004). In fact, nearly 80% of organizations use some type of electronic performance tracking (Tomczak, Lanzo and Aguinis, 2018); estimates indicate that over 26 million workers are electronically monitored (G. Stoney, 1998).

Nowadays an increasingly global workforce communicates, collaborates, and connects in global marketplaces with web- and cloud-based technologies across geographies and territorial borders (Determann and Sprague, 2011). Undoubtedly, a wide array of devices and technologies enable employers to monitor employees and track resources in order to check on productivity, safety, theft, use of company time and company resources for personal purposes, and to try to prevent harassment.

[1] This is a term often used to describe the habit of employees to use their Internet access for personal use.

Some examples of such technologies include phone tapping, video surveillance, and computer monitoring (Mishra and Crampton, 1998). Moreover, offices are often under surveillance by cameras, certain sites and social media sites are blocked on the Internet, personal data can be recorded, and electronic cards are used for employee entries and exits (Karahisar, 2014). Also, in order to control and monitor employees, employers may take additionaldiverse surveillance instruments into consideration such as *time-tracking* and *access control systems*, *e-supported systems* like chip cards, *RFID* (radio-frequency identification) chips powered by the IoT, human implants, various biometric systems, computer surveillance, network monitoring software, GPS tracking, telecommunication, visual and Internet monitoring, as well as surveillance through detective agencies (Hugl, 2013). Employers, often consider monitoring as a necessity since it increases efficiency, improves quality and ensures security.

An increasingly global workforce communicates, collaborates, and connects in global marketplaces with web- and cloud-based technologies.

Nevertheless, both the aspect of consent and that of power asymmetries, must not be taken lightly in the case of employee monitoring. According to Macnish (2015), competent adults should be able to consent to any surveillance action, so that the action itself obeys the proportionality balance between the parties involved, and hence be considered ethical. In the case of employee monitoring, the knowledge of the surveillance or monitoring is very significant. However the power asymmetries may overrule the information symmetry achieved by knowledge and consent, in case the employee is not in a powerful enough position to deny consent. In the case of SIS there are additional concerns since the monitored employees may not aware of the manipulation process of collected data.

The primary research question that will be addressed in this case study is about which ethical issues arise in the use of the selected SIS design and use, i.e. IoT-based software for monitoring and tracking and how these can be addressed.

This will be done by analysing key issues within the literature and current legislation on the topic and by conducting interviews with two software designers working for an international company, which develops and markets *on-demand and on-premise software for Subscription Billing and Rewards, which uses IoT* – CRM.COM (crm.com, 2017). The

case study further aims to identify whether software development and distribution organisations face ethical issues in IoT usage in practice, and further, if there are policies and procedures set in place for addressing these concerns; and whether they face additional issues not addressed in the literature.

This case study will first review the effects on user experience of using IoT as part of Smart Information Systems, especially systems supported by 5G networks in the near future, and will, subsequently, briefly discuss current literature and legislation relevant to such activities as monitoring and tracking (Section 2). The CRM.COM case will then focus on how the company provides tracking software as a service and as a product for businesses nationally and in several countries worldwide (Section 3). Finally, the case study will discuss the ethics of such IoT-powered software products, by considering both their design and their usage (Section 4).

2. Background Review

The background review focuses on the effects of using IoT as part of Smart Information Systems, especially systems supported by 5G networks in the near future. The effects on the users of SIS are referred to by the term Quality of Experience (QoE) and the specific effects of 5G networks on QoE are discussed in this background review. Since the user experience is also affected by such actions as employee and asset monitoring with the use of IoT, a brief overview of legal aspects related to such monitoring is given at the end of this background review. Given that employee monitoring and asset tracking is not a new topic, there are a few cases to discuss. However, the application of these practices with the use of SIS is a recent development, thus the lack of a plethora of examples.

2.1 Quality of Experience in SIS: 5G networks and IoT

Quality of Experience (QoE) of a user is an important metric to quantify how well an information system, in particular a Smart Information System, performs; and hence, its overall acceptability and usability can be assessed. Taking QoE into account, includes the complete end-to-end system; the user, the end-device, underlying network infrastructure(s), services and application/content. In order to measure QoE, it is imperative to formulate a clear understanding of what is QoE, and in turn how it can be measured. In this section we will discuss briefly the various definitions of QoE and elaborate them with respect to user experience within an Iot-aware, 5G system.

QoE is defined as, *the degree of delight or annoyance of the users of an application or service*, by the International Telecommunication Union (ITU), (International Telecommunications Union, 2017). The European Telecommunications Standards Institute (ETSI)

extends the definition to include both technical parameters and usage variables and measures both, the process and outcome of communication. It defines QoE as *a measure of user performance based on both objective and subjective psychological measures of using ICT service or product* (European Telecommunications Standards Institute, 2010). The European Network on QoE in Multimedia Systems and Services, Qualinet, defines it as; *the degree of delight or annoyance of the user of an application or service. It results from the fulfillment of his or her expectations with respect to the utility and/or enjoyment of the application or service in the light of the user's personality and current state* (Brunnström, 2013).

Extracting from these definitions, ITU has proposed two methods to measure user experience; 1) subjective QoE assessment, typically based on Mean Opinion Score (MOS) of a service according to user perception and 2) objective QoE assessment, typically involving Quality of Service (QoS) parameters like latency, traffic volume density, reliability and cost etc. (International Telecommunications Union, 2017). Also relevant to this study are the conclusions drawn by Qualinet white paper that different application domains may have different QoE requirements which can be formulated by means of influence factors and features of QoE (Brunnström, 2013). Three main Influence Factors (IF) were identified; 1) Human IFs which constitutes the physical and mental state, demographics and emotion 2) System IFs which can be related to content, media configuration, network -related and device-related and 3) Context IFs which describes the physical, temporal, social, economic and technical aspect of a user's environment (Brunnström, 2013).

*Taking**Quality of Experience** into account, includes the complete end-to-end system; the user, the end-device, underlying network infrastructure(s), services and application/content.*

The 5G technology is a networking technology that is IoT-aware, especially because the wider coverage and much faster data rates with stable connections, allow for efficient transfer of large amounts of data and support the ad hoc connections between *things* in the IoT environment. Positive user experience is crucial for technology acceptance, in particular 5G and IoT, as well as consumer willingness to pay higher service charges. In (Pierucci, 2015), it is highlighted that 5G features such as, high data rates, heterogeneous network architectures, ultra-low latency, device to device (D2D) communication, smart devices, and flexible spectrum management as challenges to QoE. Andriyanto and Su-

ryanegara (2017), argue that QoE measurements in 5G communication network should be according to the three basic scenarios proposed by ITU i.e. Enhanced Mobile Broadband, Ultra-reliable and low latency communications, and massive machine type communications. Liotou*et. al*recommends a shift from system-centric architecture to user-centric architecture for 5G ecosystem and identify some QoE requirements. They identified Software Defined Networking (SDN) as the key technology for QoE management and provisioning functions and consistecy, transparency, user personalization & service differentiation and resource & energy-efficient QoE-awareness as the key requirements (Liotou, 2015).

QoE requirements and management in a 5G network supporting IoTis further complicated by the mobility, volatility and scalability. It can be approached from multiple dimensions, application-oriented or network-oriented, further strengthened by user perspective. For this type of technology, the paradigm of mobile edge computing (MEC) within an IoT-aware, 5G network along with software defined networks (SDN) and network slicing are crucial as a significant amount of computing power will be distributed near the IoT nodes (IT Peer Network, 2018). Majority of data will be processed and stored at the network edge, which can reduce latency and provide better quality of service (and therefore better QoE) for connected nodes. By utilizing the computing power at the edge, improved real-time scheduling over the caching and transmission can be achieved, which in turn will improve the overall user experience. Considering design modifications to improve technology in terms of ethics, e.g. incorporate consent forms in new software, or model trust in data manipulation models, may occur at the edge of this network using the 5G capabilities.

2.2 Legal Issues: Employee Monitoring and Asset Tracking

The section offers some general remarks about IoT and monitoring employees, including the harm that occurs. A brief legal/human rights analysis is presented through examples from literature. The section concludes with an account on suggestions for Guidelines and policies on monitoring.

The use of monitoring technologies in the workplace is a topic which received attention from scholars and it has been addressed and touched upon from various angles. In the Internet age, as Frayer argues in his article *Employee privacy and Internet monitoring: Balancing workers' rights and dignity with legitimate management interests* (E. Frayer, 2002), employers face serious risks from employee misuse of the new communication medium (referring to emails). In fact, the tendency of employees to misuse the internet at their workplace is also confirmed through employees' testimonies in the article *Ethical Implications of Employee Monitoring: What Leaders Should Consider,* by Mujtaba (2004). Moreover, Martin and Freeman (2003) – their article will also be mentioned be-

low – hold that in 2001, 60.7% of employees surveyed said they visit Web sites or surf for personal use at work.

To reduce the risk of internet misuse in the workplace, as Frayer notes, employers are turning to new monitoring technology enabling them to view, record, and report literally everything employees do on their computers. This is one – among others (such as performance and productivity) – of the reasons for the development of the practice of monitoring in the workplace. Another reason which is mentioned by Karahisar (2014), is, as she puts it: 'in order to keep workers under pressure, to threaten, to appal, and to make them feel the power over'. More reasons for employee monitoring are mentioned in Hugl's*Workplace surveillance: examining current instruments, limitations and legal background issues* (2013) prevention of related image damage, defense of corporate espionage, a general intended protection of corporate assets, detection of illegal software and missing data, increase of productivity, detection of reasons for a disciplinary warning letter or a termination, significantly reduced costs and increased availability of surveillance technologies, and others.

Some of the many forms that monitoring in the workplace can take are discussed in *Balancing Employer Monitoring and Employee Privacy*, by Mohl (2006). Examples include monitoring e-mails to filter out inappropriate attachments or messages containing inappropriate content, Internet Web-blocking software that blocks access to non-business-related websites, as well as direct surveillance in the form of video cameras or global positioning systems.

While many employees express the view that they do not mind and/or they understand why they are being monitored, as is demonstrated in the article *Ethical Implications of Employee Monitoring: What Leaders Should Consider* by Mujtaba (2004), which is also mentioned below, this phenomenon has, among others, a psychological as well as ethical and legal dimension. Karahisar (2014), in her article *Developments in communication technologies and employee privacy in the workplace,* apart from the impact of the phenomenon on privacy, she finds that monitoring practices and controls cause pressure on employees. As she specifically writes, 'the widespread practice today is keeping employees under continuous pressure and control'. Moreover, she mentions that employer's monitoring and surveillance results in workers feeling humiliated, and may lead to stress, demoralization, and stress-related health problems in workers. Her article is based on desktop research.

Relevant to the ethical and legal dimension of the phenomenon is Karahisar's stance, thatthe case of constantly being monitored and tracked has led to the established opinion from employees that there is no privacy at work. In a similar framework, Frayer mentions that employee advocates assert that such surreptitious monitoring may infringe on employee privacy and other protected workplace rights. The feeling of invasion of the pri-

vacy of the employees is also mentioned in the article *Ethical Implications of Employee Monitoring: What Leaders Should Consider*, written by Mujtaba (2004). The issue of privacy, which is strongly connected to the IoT, is indeed important and it is also extrapolated in other articles – such as *Employee monitoring: Privacy in the workplace?* by Mishra and Crampton (1998). Beyond Karahisar, the authors of *Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses,* Chory, Vela and Avtgis (2016), examine concerns on privacy rights, due process, and fairness through an empirical study of full-time working adults' beliefs through an empirical study of full-time working adults' beliefs about their computer-mediated workplace communication privacy and their evaluations of organizational justice, trust in upper management, and commitment to the organization. Their results suggest that employees who do not perceive much privacy, tend to view their organization's policies as less fair, trust upper management less, and demonstrate less commitment to their organizations.

In Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives (Alder, (1998)), it is demonstrated through desktop research that monitoring is seen by some as dehumanizing, that it invades worker privacy, increases stress and worsens health, and that it also decreases work-life quality. In fact, monitoring employees has multidimensional effects not only on employees (their human rights, their health (including psychological), and their general well-being) and on ethics and human rights in general, but also on the business itself as it affects the way in which employees perceive their professional environment, something which can be said that it affects the performance. For example, they 'demonstrate less commitment to their organizations' as already mentioned).

Because of its legal and ethical dimension, apart from the attention from scholars, this particular practice received the attention of the legislature as well. One example which is discussed in the literature relates to Italy and is analysed in *New limits to the remote monitoring of workersactivities at the intersection between the rules of the Statute and the Privacy Code* (Alvino, 2016). In this article, Alvino examines the provisions contained in the new article 4 of the *Worker's Statute* that limits the employer's monitoring powers.

Since monitoring is a practice which can result in a violation of rights, the need for guidelines and policies on monitoring are mentioned in some articles. For example, in *Employee monitoring: Privacy in the workplace?* Mishra and Crampton, (1998) discuss the fact that employers can defuse or avoid the negative effects of monitoring, by following certain guidelines. What is more, the authors maintain that employers should undertake such activities with much forethought and care. In *Balancing Employer Monitoring and Employee Privacy*, Mohl (2006) seems to agree as he argues that *'regardless of what*

form of monitoring an employer utilizes, care must be taken to ensure that it does not violate employees' privacy rights.'

In *Employee monitoring: what are the legal issues?* (Edwards, 2015), Edwards explains what he perceives as the best advice for the employers. This is the development of a clear policy setting out when and under what circumstances an employer can undertake employee monitoring. He argues that it is important that an employer applies any policy consistently to avoid discrimination claims. He goes on to discuss how employers must ensure that their employees understand the circumstances under which the content of their emails might be monitored or reviewed. Hence, at the very least, employers should ensure that there exists a policy in place and that staff are aware of it.

Since monitoring is a practice which can result in a violation of rights, the need for guidelines and policies on monitoring are mentioned in some articles

The tension between evaluative surveillance and privacy against the backdrop of the current *explosion* of information technology is addressed by Moore (2000) in *Employee monitoring and computer technology: Evaluative surveillance v. Privacy.* Not only he agrees with Edwards above (he argues that knowledge of the different kinds of surveillance used by any given company should be made explicit to the employees) but he alsoclaims that there will be certain kinds of evaluative monitoring that violate privacy rights and should not be used in most cases.

According to Sychenko (*International Protection Of Employee's Privacy Under The European Convention On Human Rights, 2016*) the jurisprudence of the ECtHR provides a significant framework for the consideration of cases concerning employee's privacy. As is assessed in the paper. 'its broad interpretation of the right to respect for private life significantly contributed to the protection of personal data, elaborating positive obligations of the states'. The article takes into account *Bărbulescu v. Romania and presents the opinion of Dissenting Judge Pinto De Albuquerque who characterised the case as an excellent occasion for the Court to develop its case-law in the field of protection of privacy with regard to employees' Internet communications.*. Moreover, the article focuses on the Court's approach to the lawfulness and necessity of the interference with employee's privacy, as it has particular value for the employee's protection on the national level in the countries of the Council of Europe.

The recent Regulation on General Data Protection (GDPR) (2018) and its practice in Europe, makes it clear that for any employee monitoring to take place (and hence for any personal data to be collected), consent must be given by the employee. However, even

with the existence of legally compliant practices such as signed consent forms, unethical practices might do take place. For example, Macnish (2018) discusses the fact that that, even though the seeking of consent between two parties demonstrates mutual respect, reinforces autonomy and generally assures fairness, often this is not the case, since there are at least three ways in which consensual transactions might be invalidated, and they include fraud, exploitation and coercion.

2.3 Monitoring and tracking – Ethical, economic and legal dimension

In the article *Some Problems with Employee Monitoring* (Martin and Freeman, 2003)the authors identify seven key arguments that emerge from the pool of analysis regarding the ethical, economic and legal dimensions of employee monitoring. They argue that none of these arguments is conclusive and each calls for managerial and moral consideration and they conclude that a more comprehensive inquiry with ethical concern at the centre is necessary to make further progress on understanding the complexity of employee monitoring. The final section of the paper sketches out how such an inquiry would proceed.Their seven arguments have to do with productivity, security, liability, privacy, creativity, paternalism and social control.

In *Monitoring Employee Internet Usage* (Gorman, 1998), Gorman explores the question whether employers should know where their employees are going when they are provided with Internet and World Wide Web access, or if this is a breach of privacy issue.

In*Surveillance in Employment: The Case of Teleworking (1999)*, Fairweather argues that while employers have a legitimate interest in a certain amount of monitoring of their employees, an employee is not a slave. Hence, an employee should not be required to reveal their whole self to the employer but instead has a right to privacy. Fairweather argues that to allow intimate information to remain private, workers and teleworkers should not normally have personal communications under surveillance by their employer, and the employer should not routinely monitor the nature or content of a worker's home life.

While employers have a legitimate interest in a certain amount of monitoring, an employee is not a slave.

Throughout this background research into, mainly the ethical and legal issues of using Smart Information Systems (SIS) for monitoring, it becomes clear that up to now, the issue is approached more from the perspective of monitoring people. However, there is the issue of asset tracking (tracking our physical belongings, through, for example, barcode scanning, or GPS), which is more subtle but can still manipulate personal or sensitive data and support unethical practices, if not addressed early on. Both monitoring and tracking within a business have been, undoubtedly, fundamentally affected by the devel-

opment and use of SIS technology (for example, IoT) and electronic communications in the workplace. The main conclusion that can be drawn from the literature review is that there are a plethora of concerns with regards to human rights violations of employees – in particular, the right to privacy – and ethical principles. There are also many legal principles, laws and jurisprudence, which address some of these issues. Alder (1998) remarks that there are opposing opinions regarding workforce tracking and electronic performance monitoring and that both proponents and opponents of electronic monitoring fail to adequately address the arguments voiced against their point of view. A more specific, thoroughly considered and, ideally, legally binding strategy/set of rules must be created, which will allow safeguarding employers' benefits, without violating employees' rights and needs.

3. CRM.COM

CRM.COM implements and uses SIS technology within the business-to-business technology sector. The company designs and develops monitoring and tracking software that uses IoT for data collection, which is in turn sold to other businesses, either as a software product or as a service.

It is important to identify how the specific SIS is designed and implemented, as well as how it is used in practice and to evaluate if the ethical issues raised in the literature correspond to those understood and addressed in reality. In order to achieve this, the particular case study takes into consideration background research about the company, and analyses two interviews that were conducted with software designers of the company working on the IoT monitoring software. During these interviews, the interviewees' interaction with the SIS is discussed.

3.1. Description of the Organisation and Individuals

CRM.COM is an international company that, according to its website, develops and markets *on-demand and on-premise software for Subscription Billing and Rewards* (Crm.com, 2017).The specific software, which is IoT-based and focuses mostly on subscription and billing management, tracks equipment, for the purpose of deducing how assets are used in order to either bill according to their usage, or to identify usage fraud. Moreover, it is expected that there will be an increasing trend in the market share of such products in the future. The interviewees from CRM.COM, Ms.PanayiotaDemou and Mr. George Rossides, are software designers for IoT monitoring and tracking applications. They participated in two interviews, where the IoT software

CRM.COM develops and markets on-demand and on-premise software for Subscription Billing

design specifics were discussed, and furthermore, the ethics and impact of the use of such IoT tracking applications.

3.2. Description of SIS Technologies Being Used

CRM.COM explores IoT as part of their subscription and billing services and offers asset tracking services in two modes.

First, the service can host the software on a cloud server controlled by CRM.COM, and offer customers a software subscription as a service. In this case, the customer cannot completely control or have access to the software implementation and CRM.COM can monitor and maintain the software. According to the interviewees, in this case of the IoT software,

> *'we are basically using it to track the devices that consume the subscription services and to get information that might be billable'*. (George Rossides)

Second, the software can be offered as a stand-alone solution, where the software is installed at the customer's site, and thus, the customer has complete control over the management and use of the software, unless otherwise decided by the customer. In this case, even if CRM.COM supports the customer with maintenance tasks, they cannot control the software usage.

An example of software usage is given by the interviewees in the following:

> *'For example, we might have a client who gives printing machines to his customers, and based on the usage of the printing machines, the company will charge the customers accordingly. What we do is that we get this usage from the printing machines, and we bill them.'* (George Rossides)

A clarification on the data collected by the specific software was requested and the interviewees confirmed that

> *'the information that we track is information that was going to be shared with the company anyway; […] in order for the company to bill it',* (George Rossides)

and clarified that they

> *'do not track information that is not immediately needed or information that is sensitive.'* (PanayiotaDemou)

3.3. The Aims of the Organisation Designing This Technology

CRM.COM has a single IoT-related software product, which can be distributed in two modes as discussed above. Given that there is an ongoing relationship with their customers, especially, for the cloud-based tracking software, the interviewees explain that even though they can have access to the generated data, it is solely for the purpose of support and maintenance, particularly in the case of the cloud-based tracking service. With regards to the standalone solution, when the customers

> *'store it on their own server, then we do not have control over it.'* (George Rossides)

The design of the IoT software has been one of the main foci of CRM.COM during the past year. As the company operates globally, the future use is expected to be global. The company expects the market share to be either from existing customers or prospective ones, as the technology is becoming increasingly popular. Furthermore,

> *'it is not a personal judgement or a judgement made within the company – it's an area, which is actually monitored and developed by a lot of groups that we participate in, like the TM forum, a group that provides frameworks around billing, [...] and during the last couple of years they are focusing a lot on IoT'*. (George Rossides)

3.4. Limitations and Constraints of Using this Technology

With the enforcement of the General Data Protection Regulation (GDPR) in Europe, and for European citizens, since May 2018, the company needed to fulfil a number of compliance requirements. CRM.COM 's customers (businesses) have the same requirements. Software designers are also part of the compliance project:

> *'The past year we have studied the GDPR regulation in depth and we introduced several features in order to encourage our clients to comply with the regulation'*.(PanayiotaDemou)

The nature of using asset tracking technology is such that in according to the interviewees, data protection is something considered in the software design process in any case, but the introduction of the GDPR has given them an additional incentive to introduce GDPR-compliant features to the tracking software (such as consent forms and anonymity). Nevertheless, the new regulation for data protection motivated changes in the software design to enable both CRM.COM and its customers (businesses) to be compliant.

3.5. Types of Data Used

The specific tracking software is designed so as not to exploit or expose data in a way that is unnecessary or unethical, or as mentioned above, not GDPR-compliant. According to the software designers:

> *'Other than IDs and passports we don't have any sensitive information in our system up to now'.* (George Rossides)

It has been repeatedly confirmed that the software design does not consider collecting data that is not immediately needed for the billing of the customer. Therefore, the software does not track

> *'preferences of a customer, personal information of the customer or information related with the behaviour of the customer'*. (George Rossides)

So even though, tracking is done using the IoT software, the software designers incorporate as many features as possible to avoid abuse of the software during usage by their customers.

3.6. Policies Governing the Use of SIS Technology

The design and use of IoT tracking software is primarily governed by the enforcement of GDPR across Europe and for European citizens. The designers' relevant training (Section 3.4) is important, since as software designers, the interviewees always take issues of data protection into consideration, and that GDPR just added to an already existing effort:

> *'We usually take those issues into consideration when designing software for our system but once we knew that GDPR is going to be happening and taken into account, we decided to introduce some specific new features in order to help our customers comply with GDPR'.* (PanayiotaDemou)

CRM.COM supported the professional development of software designers who were educated on the new regulation, by giving them time to attend training and follow-up time, so that they can understand the different areas of the regulation. Within the company, it is understood that the GDPR is considered for revising the design of all company software and not just for IoT software (where data collection is part of the software advertised tasks).

The software includes, among its standard new features, consent forms, and monitoring of the activity by their customers relevant to the data. Regarding the consent forms:

> *'We have included it [consent] in our system. We have some states [in the software design] that will determine the functionality of each customer based on their*

consent'. (PanayiotaDemou)

Moreover, regarding the monitoring for identification of system abuse by the new owners, CRM.COM's customers (businesses):

> *'if they abuse the system to target specific cases then we provide a full audit log that can be used to trace those cases'*. (George Rossides)

However, the company does not have an official policy on how to deal with such cases at this point, although it is expected that they would take correcting actions if abuse were detected. When asked about an example of such action,

> *'It depends on the type of the abuse. It could be just to inform them to stop doing what they are doing or it could be stopping the service for them'*. (George Rossides)

3.7. The Effects on Stakeholders

ICT professionals employed in the subscribing businesses are significant stakeholders, especially once the software has been distributed to the customers (businesses). CRM.COM provides support and maintenance during the software's lifetime, which means liaison with these ICT professionals:

> *'We always provide support unless the customers request otherwise. It's the nature of our business'*. (PanayiotaDemou)

The main customers come from:

> *'IT industry and retail industry in general'*. (George)

Overall, the software can be distributed to retail companies, technology companies but can also be used in fleet management companies. These companies can be local or international, as the company operates

> *'all around the world'*. (George Rossides)

4. Ethical Issues

Throughout the two interviews conducted at CRM.COM, there were a number of ethical issues highlighted as a result of the potential use of SIS, specifically, ethical issues that arise from making use of the capabilities of IoTtechnology towards data collection, as well as from designing software for other companies to use with their own assets and resources.

These ethical issues have in large part been discussed in the interviews, matching in several cases issues highlighted by literature and legislation. Interview questions have been informed by literature and legislation in that respect. The main issues discussed include the ethics of access to the IoT-based software, issues of discrimination and equality that may arise from the use of the IoT-based software, the importance of informed consent, the potential of malicious use, issues of privacy, responsibility, as well as transparency and trust with a reference to the use of personal data by the SIS.

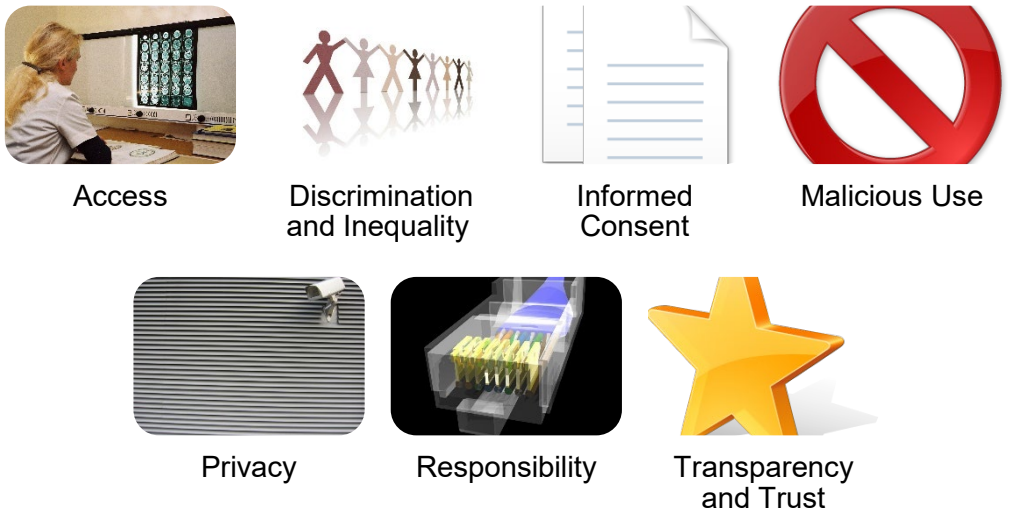

Figure 1 – Ethical issues in IoT-Based Tracking

4.1. Access to SIS

Those who have access to a software that handles data is also likely to have access to the data. Access to data handled through the IoT poses access risks, as the system is by definition connected to the Internet. Design with respect to access controls is therefore important as well as issue of consent, which we deal with below. It is not unusual that several of the identified ethical issues interconnect for a particular SIS.

The specific IoT software under consideration in this report is designed, developed and distributed by CRM.COM. Once acquired, the customers of CRM.COM use it to track or to bill their own customers. As such it is quite important to be cautious with the handling of data across the hierarchy of system users.

> *In our system, we give the ability to our customers to take consent from their customers. We give them the ability to configure how the system will work depending on the state of consent. For example, if the customer has not consented, it is not possible to allow the customer to use the system in a full functionality or even de-*

lete the customer from the system. So, we included consent.' (PanayiotaDemou)

Nevertheless, it is not always straightforward, because the system users have the technological freedom to abuse the system, e.g.

> *'they could use information to set up offers for their customers. If they want to target a specific group of customers it's up to them if they are going to do it or not'.* (George Rossides)

The question that arises is whether the software design company can do anything to control such type of access to the SIS, and the answer is that, the software is designed to trace those cases and can provide a related audit log of the software users' activity. Where access control leads to malicious use is discussed below.

4.2. Discrimination and Inequality

Discrimination and inequality were the ethical issues most dominant in the literature review, which drew mostly from cases of employee monitoring. Regarding the specific SIS under consideration for this report, this is not a major issue, as it deals primarily with asset tracking for billing.

Nevertheless, the ability of the companies that acquire the software to install it locally, and thus not be monitored by CRM.COM, avoiding any detection of potential malicious use of the system, opens the door for ethical violations by the customers themselves. In fact, the interviewees were asked whether the new owners of the software could monitor a specific group of their customer base and the CRM.COM software designers replied:

> *'Yes they could. Especially if we are talking about the billing, which is an important part of their business process.'*(GeorgeRossides)

Hence, from the capabilities of the software point of view, there is potential for discrimination of potential users of the software.

In terms of inequality, this is an issue that may arise because the access rights and permissions to the IoT software are provided to the administrators of the software within the businesses of the customers, and ultimately the access to the SIS collected data is controlled by these employees' judgement; therefore, the potential for inequality issues exists. CRM.COM provides administrators withthe ability to provide access rights to specific roles in their company so that

> *'not everyone has access to everything – it's up to the customers.'*(George Rossides)

4.3. Informed Consent

One of the main policies that has been highlighted by the enforcement of the GDPR across Europe, has been the policy of informed consent. Providing the opportunity to stakeholders to consent to the collection, manipulation, or deletion of data is very significant to ensuring data protection. CRM.COM has incorporated informed consent as a basic feature in its software:

> *'In our system, we give the ability to our customers to take consent from their customers. We give them the ability to configure how the system will work depending on the state of consent. For example, if the customer has not consented, it is not possible to allow the customer to use the system in a full functionality or even delete the customer from the system.'* (PanayiotaDemou)

Specifically, the implemented consent forms allow the product to give the freedom to the customer (business) to select the level of commitment to the software usage:

> *'we have some states [in the software design] that will determine the functionality of each customer based on their consent. We give the ability to every customer to consent themselves or to withdraw at any time. It depends on our customers how they will set up their system based on their business needs.'* (PanayiotaDemou)

Although this has been initiated as an attempt to assist their clients to be GDPR-compliant, the implementation of consent forms enhances the feeling of trust that customers have in the software. In addition to informed consent, additional implemented features enhance the levels of trust, including:

> *'the ability to anonymise customers based on specific criteria, or if the customers want to be anonymised or deleted from the system'*. (George Rossides)

4.4Potential for malicious use

Even though the technology provides for features that can encourageethical use of the system, the possibility for system abuse cannot be totally excluded. An example of abuse of the system could be that the customers (businesses) installing the system use it to collect data that can help them set up offers to their customers as a marketing technique. The software safeguards against such malicious system usage by keeping logs of activity, in order to be able to trace such cases when necessary:

> *'if they abuse the system to target specific cases then we provide a full audit log that can be used to trace those cases'*. (George Rossides)

However, there is no official policy to address such behaviour. The actions that will be

taken in case malicious use of the system is detected, varies:

> *'It depends on the type of the abuse. It could be just to inform them to stop doing what they are doing or it could be stopping the service for them'*. (George Rossides)

The interviewees elaborated on risks of abusing the software, especially if such software is not designed or implemented correctly. Such risks may include

> *'breach of personal data, malicious software coming into your personal device… those kind of things'*. (PanayiotaDemou)

Adopting the design of mechanisms such as consent forms and anonymization of data in the IoT software ensures a level of security towards the customers (businesses), as well as their own customers. Moreover, encryption in communicating the generated data also safeguards against the malicious use of such data; for example, in the case that data is maliciously eavesdropped or intercepted by third parties:

> *'All the information which is exchanged between the systems is encrypted'*. (George Rossides)

4.6. Privacy

IoT is by its very nature susceptible to privacy breaches as it has been used in businesses to monitor and track users and their environment, without the need for human intervention. According to the interviewees,

> *'When it comes to the IoT, we are basically using it to track the devices that consume the subscription services and to get information that might be billable.'* (George Rossides)

Furthermore, the IoT software is used to track the customer (business) in order to assess billing capabilities:

> *'We are tracking the customer. For example, we might have a client who gives printing machines to his customers and based on the usage of the printing machines, the company will charge the customers accordingly. What we do is that we get this usage from the printing machines and we bill them'*. (George Rossides)

Considering the collection of data is necessary to continue with billing, the software is designed not to collect any sensitive information, although some personal information is collected for identification purposes:

> *'Other than IDs and passwords we don't have any sensitive information in our system up to now. This is anonymized if the customer requires we retrieve'.* (George Rossides)

The matter of anonymising the information is significant to ensure that the information cannot be used maliciously if retrieved or intercepted without the appropriate permissions. This anonymization policy is also supported by the software design and use in terms of data storage and generation of usage logs:

> *'We don't keep this information. We have a full anonymization. We don't keep personal data in the logs, e.g. passwords'*. (George Rossides)

Being questioned whether the customers of CRM.COM are aware of the generation of logs, the interviewees claimed that they,

> *'have included specific clauses in [their] contract with [their] clients so that they know that we have access and if they have their own log enabled they will check where our users logged into and what they've seen.'* (George Rossides)

Moreover, the access to the software for support and maintenance, including access to the data and activity logs, comes with the service that CRM.COM provides, although the customers themselves often have the opportunity to deny access to collected data from their side of operations:

> *'We always provide support unless the customer requests otherwise. It's the nature of our business. We don't have a process to ensure that we don't have access to sensitive information during maintenance but of course, if a customer requests it then the access is removed from their side. It is usually up to the customer because they provide access to us and not the other way around'.* (George Rossides)

From the narrative above, we have already identified that according to the interviewees, in addition to data necessary for billing, e.g. asset's consumption, the only items of personal data collected are IDs and Passwords for identification purposes, although all data is anonymised prior to being stored. The names are retrievable, though, through a process known as pseudonymisation, which allows the original data to be retrievable upon request:

> *'this is anonymized, if the customer requires we retrieve. We don't keep this information. We have a full anonymization. We don't keep personal data in the logs, eg passwords.'* (George Rossides)

It is useful to note here, that both anonymization and pseudonymisation are acceptable from a legal perspective as GDPR mechanisms for preventing personal data exposure, and that the interviewees are clearly aware of this.

4.8 Transparency and Trust

Transparency of software design and handling is an important aspect, especially when transparency points to open source software. Transparency increases the likelihood of identifying any biases in the software design and development. In private organisations, the practice of open source software is not possible due to the competitive nature of the market and thus transparency capabilities or opportunities are important to the user for privately developed software. This is especially significant when a data collection process is established by the software and trust is required on behalf of the customer that no personal or sensitive data will be exposed.

The mechanism concerned with such issues of trust and transparency in the design of the IoTsoftware under consideration in this report is the use of logs to capture the activity:

> *'we provide a full audit log of which users did what and when reporting of those actions*'. (George Rossides)

In the spirit of transparency, the customers are made aware of this mechanism:

> *'we have included specific clauses in our contract with our clients so that they know that we have access and if they have their own log enabled they will check where our users logged into and what they've see'*. (George Rossides)

The customers can of course stop this:

> *'if a customer requests it then the access is removed from their side. […] It is usually up to the customer because they provide access to us and not the other way around'.* (George Rossides)

Although the mechanism is there to support transparency and trust it is not a feature that can be enforced upon the customers to use, same as consent forms.

5. Conclusion

This IoT case study introduced an IoT-powered software for asset tracking, a process that requires live data collection including personal data. The software design process in this case requires to consider relevant legislation, responsibility issues and delivery and support of software. Despite the attempts made within the software design and development phases to incorporate as many features as possible to promote the software's ethical and responsible use, there are still a number of ethical issuesthat need to be addressed when theIoT SIS technology is used by its users, e.g. privacy, transparency and trust; often businesses themselves (e.g. retail or technology businesses) that can use it to track their own customers and employees.

The interviews with two software designers from CRM.COM offered perspectives into the design and development policies and guidelines, the methods of considering legislation within the software design process and the ethical risks in the use of such a technology. During the interviews a number of practical, organisational and ethical issues were addressed such the ethics of access to the SIS, specifically the IoT-based software, potential ethical issues of discrimination and equality, that may arise from the use of the SIS, the importance of informed consent, especially with the enforcement of GDPR across Europe, potential of malicious use of the SIS in its current form, issues of privacy, etc.

Responsible software design and consequently a software that incorporates features of such responsible design is the desired outcome of any software product. The enforcement of the GDPR further elevated the significance of responsibility within the software design process to ensure ethical and unbiased data handling and use. The interviewees suggested that the GDPR was indeed a reason for more responsible software design but they also pointed out:

> *'We usually take those issues into consideration when designing software for our system but once we knew that GDPR is going to be happening and taken into account, we decided to introduce some specific new features in order to help our customers comply with GDPR'. (PanayiotaDemou)*

The design and use of the software is thus susceptible to human discretion. Appropriate policies and employee training could be steps to improving this challenge.

5.1Limitations

In addition to the particular aspects of the use of IoT in software design and development for tracking applications, which have been highlighted in the report, there still exist certain limitations of the product design and use that the company can address in the future. Specifically, there is currently no formal policy to dictate the actions to be taken in case of system abuse, once the abuse has been detected using the system logs. The abuse refers to violations of ethical principles in terms of misusing collected data, for instance, to further the company's marketing campaign. Even though the mechanisms are in place to capture such behaviour, the company has no official policy on how to act once such behaviouris detected.

Another limitation is that the administrators of the software in case of standalone installations on local servers can solely control access to the system. The administrators, in this case, are employees of the customer businesses and the company that developed the software has no monitoring access to the logs unless given by the administrators. The administrators also can assign permissions to the use of the software at their own discre-

tion. To avoid using the software according to the discretion of each user, appropriate policies and/or employee training could overcome the specific limitation.

5.2Contribution to knowledge

Overall, the area of using IoT-based tracking and monitoring applications to assist and enhance specific business processes is growing and becoming increasingly popular, both in terms of development and use. Being a new research area, however, it lacks sufficient literature that examines the ethical, social, economic and legal implications of the use of this technology. Such studies into the design, development and use of such IoT-based applications present important relevant information that enriches the state-of-the-art literature on the topic both from an academic and a practical perspective.

5.3Implications of this report

This report offers an original case study on the use of an IoT related SIS in the software design and development area. From the extensive research on the topic presented mainly in section 1, it is evident that there has been very little research conducted in the application of the specific SIS in industry. Academically, the issue of IoT usage has been investigated vigorously, however, the tracking and monitoring aspects and their theoretical implications, when using this technology, is limited. Conversely, many of the ethical and legal issues discussed in this report have been analysed more generally within academia and assessed in other areas of application, but have rarely been associated with the IoT usage for tracking and monitoring. Therefore, this report will be highly valuable for the development and furthering of theory, knowledge and application for designing, developing and using such IoT based applications.

5.4Further Research

The report presented considerations for the design and development of software applications based on IoT technology that can be used by businesses (e.g. retail) for tracking and monitoring purposes, in order to improve their business processes' efficiency. However, the use of IoT and the related data collection raises certain ethical considerations that must also be taken into consideration. The specific software is in fact, designed to capture some of these concerns by incorporating data protection friendly features such as consent forms, encryption and anonymity capabilities. Further research would need to validate that the use of the software with these features overcomes initial ethical concerns, otherwise software design methodologies should revisit the design in order to address any remaining issues. Relevant proposed training at a business level should also be addressed by future work, as well as consequent policy at a more global level, since the use of such software is only expected to increase in the future.

6. References

Alder, G. S. (1998). *Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives*, Springer Business Ethics, 7 (17), pp. 729 – 743.

Alvino, I. (2016). New limits to the remote monitoring of workers' activities at the intersection between the rules of the Statute and the privacy Code. *Labour& Law Issues,*, 2(1), pp.1-45.

Andriyanto F. &Suryanegara M. (2017). The QoE Assessment Model for 5G Mobile Technology.

Atkinson, J. (2018). Workplace Monitoring and the Right to Private Life at Work. *The Modern Law Review*, 81(4), pp.688-700.

Brunnström, K., , et al. (2013). Qualinet White Paper on Definitions of Quality of Experience. hal-00977812

Cheng, P., Liu, D. and Jiang, C. (2010). Monitoring employee activity without infringing privacy laws. *China Staff*, 16(1), pp.24-27.

Chory, R., Vela, L. and Avtgis, T. (2016). Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses. *Employee Responsibilities and Rights Journal*, 28(1), pp.23-43.

Crm.com. (2017). *Who We Are*. [online] Available at: http://www.crm.com/company/who-we-are [Accessed 2 Nov. 2018].

Determann, L. and Sprague, R. (2011). Intrusive monitoring: employee privacy expectations are reasonable in Europe, destroyed in the United States. *Berkley Technology Law Journal*, [online] 26(2), pp.979-1036. Available at: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1899&context=btlj [Accessed 2 Nov. 2018].

E. Frayer, C. (2002). Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests. *The Business Lawyer*, [online] 57(2), pp.857-874. Available at: https://www.jstor.org/stable/40688047 [Accessed 2 Nov. 2018].

Edwards, G. (2015). Employee Monitoring. What are the Legal Issues?. *Credit Management*, p.49.

European Telecommunications Standards Institute. (2010). ETSI TR 102 643: Human Factors (HF) Quality of Experience (QoE) requirements for real-time communication services. [Online]. Available: http://www.etsi.org

Fairweather, N., B. (1999). Surveillance in Employment: the Case of Teleworking, *Journal of Business Ethics* ,22(1). Pp. 39-49.

G. Stoney, A. (1998). Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives. *Journal of Business Ethics*, [online] 17(7), pp.729–743. Available at: https://link.springer.com/article/10.1023/A:1005776615072 [Accessed 5 Nov. 2018].

Gorman, J. (1998). Monitoring Employee Internet Usage. *Business Ethics: A European Review*, 7(1), pp.21-24.

HR Focus (2013). High-Tech Tracking: Good Business Practice or Orwellian Nightmare? May 2013, 90(5).

Hugl, U. (2013). Workplace surveillance: examining current instruments, limitations and legal background issues. *Tourism & Management Studies*, [online] 9(1), pp.58-63. Available at: http://www.scielo.mec.pt/pdf/tms/v9n1/v9n1a09.pdf [Accessed 6 Nov. 2018].

International Telecommunication Union. (2017). ITU-T P.10/G.100 Vocabulary for performance, quality of service and quality of experience. [Online]. Available: http://www.itu.int.

IT Peer Network (2018). Paving the Way to 5G with Edge Computing and Network Slicing. Intel Corporation.

Karahisar, T. (2014). Developments in Communication Technologies and Employee Privacy in the Workplace. *Journal of Media Critiques*, 1(3), pp.221-234.

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. Telecommunications Policy, 38(11), 1134-1145. doi: 10.1016/j.telpol.2014.10.002

LASPROGATA, G., J. KING, N. and Pillay, S. (2004). Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada. *Stanford Technology Law Review*, [online] 4. Available at: https://www.sukanyapillay.com/wp-content/uploads/Regulation-of-Electronic-Employee-Monitoring.pdf [Accessed 1 Nov. 2018].

Liotou, E. (2015) Shaping QoE in the 5G Ecosystem, 7th International Workshop on Quality of Multimedia Experience (IEEE QoMEX)

López, R. and Schwarz, R. (2017). Corporate monitoring by technological means in Spain: overview of substantive and procedural conceptual construction. *JURIS - Revista da Faculdade de Direito*, 27(1), pp.11-48.

Madakam S, Ramaswamy R, Tripathi S (2015) Journal of Computer and Communications, 3, 164-173, at: https://file.scirp.org/pdf/JCC_2015052516013923.pdf

Macnish, K. (2018) *The Ethics of Surveillance: an introduction*. Routledge: London.

Macnish, K. (2015). An Eye for an Eye: Proportionality and Surveillance, *Ethical Theory and Moral Practice* 18, no. 3 (2015): 529–48, doi:10.1007/s10677-014-9537-5.

Martin, K. and Freeman, R. (2003). Some Problems with Employee Monitoring. *SSRN Electronic Journal*, 43(4), pp.353-361.

Miedema, A. and Pushalik, A. (2009). *How, and when, employers should monitor employees*. [online] Hrreporter.com. Available at: https://www.hrreporter.com/article/7295-how-and-when-employers-should-monitor-employees/ [Accessed 6 Nov. 2018].

Mirchin, D. (2012). Monitoring Employee Online Activity. *Information Today*, 29(2), pp.32-33.

Mishra, J. and Crampton, S. (1998). Employee monitoring: Privacy in the workplace?. *Advanced Management Journal*, [online] 63(3), pp.4-14. Available at: http://faculty.bus.olemiss.edu/breithel/final%20backup%20of%20bus620%20summer%202000%20from%20mba%20server/frankie_gulledge/employee_workplace_monitoring/employee_monitoring_privacy_in_the_workplace.htm [Accessed 4 Nov. 2018].

Mohl, D. (2006). Balancing Employer Monitoring and Employee Privacy. *Workspan*, pp.68-70.

Moore, A. (2000). Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy. *Business Ethics Quarterly*, 10(3), pp.697-709.

Mujtaba, B. (2004). Ethical Implications of Employee Monitoring: What Leaders Should Consider' Journal of Applied Management and Entrepreneurship. *The Journal of Applied Management and Entrepreneurship*, 8(3), pp.22-47.

Personnel Today. (2006). *Employee monitoring - Personnel Today*. [online] Available at: https://www.personneltoday.com/hr/employee-monitoring/ [Accessed 6 Nov. 2018].

Pierucci, L. (2015) The Quality of Experience Perspective toward 5G Technology, in IEEE Wireless Communications Proceedings.

Sychenko, E. (2017). International Protection of Employee's Privacy under the European Convention on Human Rights. *ZbornikPravnogFakulteta u Zagrebu*, 67(5), pp.757-781.

Tomczak, D., Lanzo, L. and Aguinis, H. (2018). Evidence-based recommendations for employee performance monitoring. *Business Horizons*, 61(2), pp.251-259.

Tournier, B. (2017). *IoT-Enabled Asset Tracking is Driving Business Innovation*. [online] Sierrawireless.com. Available at: https://www.sierrawireless.com/iot-blog/iot-

blog/2017/09/iot_enabled_asset_tracking_is_driving_business_innovation/ [Accessed 8 Nov. 2018].

Yerby, J., (2013). Legal and Ethical Issues of Employee Monitoring, *Online Journal of Applied Knowledge Management,* 1(2), pp. 1 – 55.