LUND
UNIVERSITY

Ethics and the Internet of Things (IoT)

How Ethical Principles are Communicated between law, academia and the development of the IoT.

Joakim Marklund

Lund University

Sociology of Law Department

Master Thesis (SOLM02)

Supervisor: Jannice Käll

Examiner: Matthias Baier

Abstract

As the Internet of Things (IoT) becomes more and more prevalent, there are growing concerns of how it will affect our lives. With its capabilities to record large amounts of data, it carries large risks to personal privacy and the protection of our personal data. The opacity of IoT also makes it hard to know exactly what data is being collected and how it is protected, as such transparency and security are also major concerns. Legislation such as GDPR are meant to protect these ethical principles. At the same time a lot of research is being done both pertaining to the risks as well as proposed solutions. However, it remains unclear if the legal system and the academic system are able to communicate these principles to the people developing IoT. With Niklas Luhmann's systems theory as a theoretical backdrop, this thesis is using semi-structured interviews to explore the way these ethical principles are communicated between the system of IoT development, the legal system and the academic system. Finding that there are issues with how they are communicated between the system as well as how the differences in the binary code of the different systems causes friction when the principles are to be translate from one system to another. While the legal system can communicate its ideas the academic system fairs much worse. In the end, the communication needs to match the binary code of the system of IoT development for successful communication to occur.

Keywords: Internet of Things, IoT, Privacy, Transparency, Security, Luhmann

Contents

Introduction

Most people have not heard of the Internet of Things (IoT), but it is rapidly becoming one of the most important technological developments in our lives. Some scholars even suggests that its impact on our lives will be greater than both AI and automation (Nord, Koohang, & Paliszkiewicz, 2019). And like with other technological developments there are many ethical concerns especially concerning safety, privacy and transparency. As IoT works between things and gathers, transfers and act upon large amounts of information, how can we know that our privacy is secured and that the data we are willing to give up is kept from malicious actors? With the EUs General Data Protection Regulation (GDPR) we have some legal protection, but is it enough and how is it used by the people developing IoT?

AI has, for good reasons, been a concern for major discussions in the last few years. With the development of AI chatbots such as Chat GPT we are beginning to see some early signs of just what AI may be capable of. The IoT has however fallen to the wayside. Most people will not even know what it is unless they are working with it. It is however not necessarily separate from AI as many IoT devices are likely to integrate AI into them. While the risks of AI are mostly digital, IoT will bring them out into the physical world by becoming the nervous system and senses of the brain that is AI affecting not just the digital world but the physical as well.

IoT systems are often meant to be built into a network of IoT in things such as smart cities. These networks will have access to very large amounts of diverse data. As such, there may be concerns that the developers in individual projects are not seeing the forest for the trees and simply focus on the ethical implications of their own projects. But what will happen when all the individual trees eventually become a forest, is there enough consideration and protection to protect our privacy even when so called “big data” is collected on us? With the development of social media platforms, it is clear that legislation has fallen behind and has not been able to keep up with the rapidly increasing threats to our privacy and our rights. Unless we want to make the same mistake again with regards to IoT, it is important that we get ahead of the curve and take these issues seriously and try to preempt the issues that may arise in the future. Hopefully it is not too late.

Background

The most commonly used definition for the internet of things comes from the International Telecommunications Union (ITU) and states as following:

> *"A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies." (ITU-T, 2012, p. 1)*

And by 'thing' in this context they mean and object that is either part of the physical or information world, meaning either a physical or a virtual 'thing'. (ITU-T, 2012, p. 1). In essence it is the internet for objects without the need for a human acting as a mediator. While the term 'internet of things' has been around since 1999, we have for decades used computers and networks for monitoring and controlling devices (Rose, Eldridge, & Chapin, 2015, p. 7)

The Internet Society (2015) describes four different communications models for IoT. *Device-to-device* communications where devices can communicate directly with each other to perform their function (Rose, Eldridge, & Chapin, 2015, p. 13). Examples of this are devices in your home, connected to wi-fi, that you directly control via an app in your phone. Could be things such as fans, lights, or speaker systems. The second communications model is *device-to-cloud* communications where you have an application service provider that serves as an intermediary (Rose, Eldridge, & Chapin, 2015, p. 14). An example of this is an alarm system in your home that you can control remotely using an app in your phone, where the alarm provider is acting as the intermediary. Next communications model is the device-to-gateway model where IoT devices connect to the cloud via an application-layer gateway (ALG). The device then uses the ALG as a conduit to connect to the cloud because the device itself is incapable of doing it alone (Rose, Eldridge, & Chapin, 2015, p. 15). An example is home appliances that uses a hub unit to connect to the internet such as the alarm system from the earlier example, could have cameras and sensors that connect to a main hub, which in turn is connected to the internet and reaches the cloud from there. Lastly there is the *back-end data-sharing model* where users can collect data from cloud services in combination with data from other sources (Rose, Eldridge, & Chapin, 2015, p. 16). En example could be if someone is in control of several buildings which each has sensors collecting data from things such as thermostats and humidity detectors and want to access the data from all the buildings at once.

At its most basic form IoT consists of three layers a perception layer, a network layer and an application layer (Chanal & Kakkasageri, 2020). The perception layer will consist of

detection devices such as cameras or sensors that then will communicate with other devices through a network like the internet (network layer), the application layer then consists of devices that act upon the information transmitted. A very simple example could be a motion sensor in a building detecting a burglar that then sends a signal to a police computer that tells the police that there has been a break in. More advanced forms of IoT could encompass an entire city where traffic sensors, cameras, GPS systems and historical data will use AI to predict the flow of traffic and automatically redirect traffic using traffic signals to reduce congestion and maximize efficiency. This would be part of what is commonly called the "smart city".

Because IoT is used to collect data and has the capacity to collect very large amounts of data on people, naturally there are privacy concerns as to what type of data can be collected, how it is being handled and who has access to it. IoT is also notoriously susceptible to hacking and are often subjected to hacking attempts which raises security concerns as well as further privacy risks (Nord, Koohang, & Paliszkiewicz, 2019). Since IoT consists of communication between devices without human interference, most of the actions of any IoT network will remain hidden from sight. As such, the importance of transparency as to how we are being monitored and how our data is being used is of utmost importance.

IoT has increasingly raised concerns as to the way it may affect our privacy and how there are risks associated with its very broad surveillance capabilities (Hydén, 2020).

Technology and Ethics

Ever since the internet started to become a part of our lives, there has been concerns about ethics surrounding technology, especially regarding privacy. Questions such as: who has access to our e-mails, how secure are the pictures that we upload to the internet, and who can see what I write to my friends or hear what I say have always existed in the back of people's minds. Lawrence Lessig (2006) wrote on the topic of privacy, comparing it to companies' reaction to copyright infringement, saying that the convenience of the technology means that we have to pay a price in the form of parts of our data (Lessig, 2006, p. 200). Continuing, argued that one of the issues regarding privacy in the age of the internet is that we have had to rethink what privacy actually means. Whereas the old form of privacy was 'private privacy' in that we would have privacy in our homes, protected by four walls, with the internet moving into our homes and our private data moving into the domain of technology, that form of privacy became insufficient (ibid, p. 201).

Aim and Purpose

This thesis aims to use semi-structured interviews to uncover how communication works between the system of IoT development, the legal system and the academic system. Using Luhmann's theory of autopoietic systems (Luhmann, 2013).

Specifically the purpose is to see how the ethical principles of privacy, transparency and security in relation to IoT is communicated between the systems.

There are laws and legal guidelines especially from the EU that covers things such as data protection, camera surveillance and privacy intrusion. But, how do these laws work in practice, are they enough and are they communicated properly so that the people using them for guidance understand them and can clearly know how to interpret them? Or are the laws perhaps too restrictive and get in the way of important developments?

There are also innumerable academic papers written around these issues with regard to IoT, which could offer guidance to the development even beyond what the legal arena is capable of. Very little research has been done as to how these productions are communicated to the relevant recipients. As such, interview's have been conducted with managers of IoT projects around Sweden too attempt to uncover the communication of these ethical principles.

To this end the following research questions will be the basis for this thesis:

- How do managers of IoT development projects view privacy, transparency and security?
- How are these principles reflected in the legal and academic systems?
- How are these principles communicated between the academy, the legal system and developers?

Niklas Luhmann's systems theory will act as a theoretical framework when analyzing these questions. The focus on communication make it a natural fit. It will allow for a view of each part as individual systems granting the advantage of viewing the system of IoT development as its individual system with each project as subsystems within the system. In this way it is possible to explore the communication both between the systems, within the systems as well how the communication may differ depending on the positioning of each subsystem.

Delimitations

Luhmann is often considered a radical constructivist. The way Luhmann justifies his constructivist approach is by arguing that the objective reality is far too complex to properly be observed (Luhmann, 2013, pp. 120-121). There are many ways to envision the cause to the perception of ethical principles held within a system. For example, the system of IoT development is likely partially influenced by any number of different systems within its environment: legal; academic; socio-political; economic; technological; societal… the list could go on and on. As such, considering the scope of this thesis some delimitations must be drawn. As a sociology of law thesis, the two systems most readily available are the legal system and the academic system. These systems are also appropriate due to the contemporary concerns surrounding technological development, with the academic system being at the forefront of ethical implications and the legal system often argued to be falling behind. As such this thesis will focus on these two systems and their communication with the system of IoT development.

Regarding the choice of ethical principles these will be limited to privacy, transparency and security. While there are others that would be of interest such as access, equality or representation, the nature of IoT with its detection capabilities makes privacy a major concern (Hydén, 2020). With the prevalence of GDPR and its focus on privacy it is the most appropriate principle. Transparency and security are also tightly connected to privacy. Transparency regarding how data is collected and stored and security regarding how the data is protected.

Theory

Luhmann's systems theory will act as the theoretical framework of this thesis. As the purpose of the thesis is to analyze ethical principles as communication between systems, Luhmann's version of communication is the most appropriate choice.

Systems Theory

The way Niklas Luhmann's systems theory will be applied in this thesis is by viewing the law, the academy and IoT development as social systems. However, mainly IoT development will be viewed as a system and the other two will be viewed as part of that system's environment.

According to Luhmann there are three different kinds of systems: *biological*, *psychic* and *social* systems (Luhmann, 2013, p. 28). An example of a biological system could be the

human body with its internal operations, while the mind would be an example of a psychic system. Since biological systems belong to the domain of biologists and psychic systems the domain of psychiatrists and psychologists, as a social science thesis the focus will be on social systems. Examples of social systems could be a legal system, a political system, a company, an organization or just about anything that functions on a social basis.

Open Systems, Operationally Closed

The way that Luhmann defines systems is as difference, that is difference between system and environment (Luhmann, 2013, p. 44). In order to understand what this means we have to establish the boundaries between the system and the environment. The boundaries are defined by the systems operations, that is the production of the system itself (Luhmann, Introduction to Systems Theory, 2013, p. 64). The system thus draws the distinction between itself and the environment through its operations. Through the operations the system then reproduces itself, meaning that all systems are self-reproducing systems (Luhmann, Introduction to Systems Theory, 2013). The system also self-organizes through its operations which is what gives the system its structure, as a system is nothing but its operations (Luhmann, Introduction to Systems Theory, 2013, p. 70). A system can either be open or closed. A closed system is reproducing itself only through self-reference and is unaffected by the surrounding environment while an open system is open to influence by the environment. According to Luhmann, systems necessarily need to be open as they would dissipate through entropy if they were closed as they could not develop or adapt (Luhmann, 2013, p. 64). While the system itself is open, it is however, operationally closed, meaning that only the system itself can perform its operations and only the system can reproduce itself (Luhmann, 2013, pp. 63-65).

Communication

The way that a system can remain open to its environment but at the same time remain operationally closed is through communication. The way that Luhmann describes communication differs from how communication is typically described. He states that communication happens in the form of *information*, *utterance* and *understanding* (Luhmann, 2013, p. 53). To explain this, we first need to understand what Luhmann means by *information*. He describes information as "*a difference that makes a difference*" (Luhmann, 2013, p. 91). What he means by this is that when we select something as information, we differentiate it from everything that is not that information. As such it is a difference from everything else. In order for it to be information it also needs to make a difference for the operations of the system

(Luhmann, 2013, p. 46). In the context of systems, *utterance* means creating an irritation that the system must respond to. This irritation can be created by something in the environment or within the system itself. The system then observes the irritation and decides whether it is compatible with its operations. If not, it disregards it as it cannot understand it. If it is, it will integrate it with its operations as it reproduces itself (Luhmann, 2013, pp. 53-54). The system observes both itself and its environment. According to Luhmann there is no difference between observation and self-reference as in order to observe something it has to be done as a differentiation of the self (Luhmann, Introduction to Systems Theory, 2013). The system will thus simultaneously observe itself and its environment, which Luhmann describes as self-reference and hetero-reference (Luhmann, 2013, p. 56). With this information the system then understands what is compatible with its operations and reenters itself with that information to conclude the communication. As such communication always and only happens inside of the system.

As this is rather abstract here is an example of how this could work within the context of IoT development. Let us say that a Swedish municipality has a problem that it needs to solve. If the IoT development system is able to observe the problem, it will create an irritation in the system. The system will then decide if the problem is compatible with its operations or not. If the problem is that new schools need to be built, the system will disregard the problem as it cannot understand the problem due to it not being compatible with the operations of IoT development. If instead the problem is that the computer systems of various parts of the municipality are not integrated with each other and cannot cooperate properly, then perhaps there may be an IoT solution. The system may then determine that the problem is compatible with its operations. As it reproduces itself it starts adjusting to the specific needs of the project. Then in turn the system can apply for funding with an institution like Vinnova, which is the system sending out an utterance as an irritation in its environment. In turn, Vinnova's system needs to respond to this. If the needed funds are granted, the system again may deem it compatible with its operations and reproduce itself to start the project. If the granted funding is lower than what was asked for, the system may or may not deem it compatible with the operations and adapt or disregard it. This happens constantly and simultaneously within each system.

Autopoiesis

Most of what is contained within the concept of autopoiesis has already been covered above. However, it is such a central concept of systems theory that it may be necessary to explicitly explain it. *Autopoiesis* consists of *auto* meaning self and *poiesis* meaning production. Thus, it literally translates to self-production (Luhmann, 2013, p. 78). In Luhmann's system theory all systems are so called autopoietic systems. What this means is that they consist of only their operations. Their operations at the same time produces the system itself (Luhmann, 2013, pp. 63-64). As such, the system is in a constant state of self-reproduction.

Structural coupling

As stated above, Luhmann defines the system as a differentiation between system and environment. What this means in essence is that anything that lies outside of the operations of the system could be seen as part of the environment. The way that the system is able to sift through the 'noise' of the environment is through what Luhmann describes as *structural coupling* (Luhmann, 2013, p. 69). What this means is that the way in which the system has organized its operations couples it with parts of the environment (Luhmann, 2013, p. 83). It is through this coupling that the environment enacts influence on the system. The environment however cannot act upon the autopoiesis of the system, as the environment can only act through irritation and as such only has destructive capabilities as it pertains to the system (Luhmann, 2013, p. 85). This means that the environment has the capability to destroy the system but does not have the capacity to produce anything inside of the system that is the domain of the operations of the autopoietic system itself. Only after the destructive irritation of the environment is understood by the system, can the system transform the irritation into information and produce its operations (Luhmann, 2013, p. 91).

An example of how structural coupling could work is how the legal system is structurally couple to many social systems in society. All other systems necessarily need to respond to any irritation that the legal system creates within their environment. Take the example of IoT development: if a new law is produced within the legal system that has an influence on IoT development, the law can be so restrictive that it makes IoT development impossible. Thus, the legal system destroys the system of IoT development. If, however, the legal system produces a law limiting invasion of privacy, the parts of IoT development that would come into conflict with that law are essentially destroyed. The system then needs to adapt its structure so that the operations do not come into conflict with that law. As such, the legal system and the system of IoT development are structurally coupled. In this way the legal

system can only destroy the system of IoT development and any production must come from the systems operations.

Luhmann also emphasizes that the structural coupling can cause changes within the system as an anticipated response to something within another system (Luhmann, 1991, p. 1424) For example, a system structurally coupled with the legal system may adapt to what it expects from the legal system, regardless of the actual actions of the legal system (ibid.)

Observation and The Observer

Lastly, we need to address the role of the observer and observations as it pertains to systems theory. Observation is very central to Luhmann's theory, it is how the system communicates and interacts with its environment (Luhmann, 2013, p. 102). As stated above, according to Luhmann, there is also no difference between observation and self-reference. As such, observation is also central to autopoiesis.

Seeing how central observation is to systems theory, naturally, the observer become very important as well. Within systems theory all systems and individuals have are potential observers. It is important to note that the observer is never separate from either the systems or their environment but themselves exist within a context. Because observation is self-reference whether it is a system that is observing or an individual, the observation will always be done with reference to the self or the context in which the self exists (Luhmann, 2012b, p. 10). Furthermore, the position of the observer as it pertains to observing systems can either be internal or external, meaning that the observer can either be within the system or observe it from the outside. As Luhmann describes it, the boundaries of the system and its environment as well as the causalities within the system is dependent on the observer at any given moment (Luhmann, 2012b, p. 90). As such, the observer can see things as part of a systems environment that the system itself may not be able to observe and can also see the system as operating in certain ways that may differ from another observer (Luhmann, 2013, pp. 103-104). Pertaining to causalities, what Luhmann means is that there are an almost infinite number of causes to any single effect, depending on how you contextualize it. As such, it is impossible for the observer to see all the causalities as causes (Luhmann, 2012a, p. 271). Therefore, whenever a cause is ascribed to an effect it is contingent on what the observer views as the cause of said effect (Luhmann, 2013, p. 65). Say for example, that a new law comes into effect that requires a certain level of transparency within IoT. Afterwards an IoT project, creates a new IoT solution and are meeting the transparency requirements of the law. As an observer we can say that the

cause of the IoT project meeting the requirements of the law may be the new law. But we could also say that the cause was whatever caused the law to be written, for example a public demand for more transparency. As the developers of IoT are part of the public, it is also possible that they share that very same concern and that they simply use self-reference, and the cause is therefore their own values. It could be all these things or, perhaps, something that we as the observer cannot see. As such the causes of the effect are contingent on us as the observer, both as it pertains to what we can observe and to what we ascribe as the cause.

This thesis is engaging in something Luhmann calls second-order observation. Meaning an observation of an observation (Luhmann, 2013, pp. 111-112). As this thesis means to see how the various systems are observing each other and ascribe a causal link on how ethical values are communicated. As stated above however, the observer is never separate from everything. As such, it will be important moving forward to consider the position of the observer. As academics we are part of the academic system, meaning that this second-order observation is as part of one of the systems being observed and therefore uses that system as the self-reference for the observation.

Defining the Systems

Legal System

Luhmann has written extensively about the legal system and this thesis will not deviate from his views on it (Luhmann, 1991). The legal system is just as most people will view it, the laws, regulations, courts etc. that we typically refer to as a legal system. The distinction that makes up the internal communication of the legal system according to Luhman is between legal and illegal (Luhmann, 1991, p. 1428). This means that whatever the legal system integrates into itself needs to be translated into this specific distinction, it is the only way the legal system can internally observe it (ibid.). This is also how the system distinquish itself from its environment. If a determination between something being legal or illegal appears at any point it will always be part of the legal system (ibid.).

Academic system:

While Luhmann has mentioned the academic system a few times (Luhmann, 1991, p. 1430), descriptions and definitions of it are hard to find. As such, for the purpose of this thesis,

the academic system would include anything that is produced by the academy, the universities, students, scientific journals and papers etc.

In the same way as the legal system, the academic system needs to be defined by its own internal binary distinction like legal and illegal. The question is how this distinction should be drawn. The academic system fundamentally is treating knowledge and the transference of knowledge. As such, the academic system's distinction could be envisioned as transferable and non-transferable knowledge. However, as the operations of the system need to be autopoietic and assist in the maintenance of the system itself a more appropriate distinction would be marketable knowledge and non-marketable knowledge (Luhmann, 1991, p. 1420). However, this distinction becomes very broad and would include things such as new papers. As such the working distinction will be academic and non-academic knowledge. Where academic knowledge is knowledge that is marketable to publishers, journals and students. While this definition becomes somewhat circular, it is sufficient for the purpose of this study. As it both distinguishes the academic system from its environment, and it also is in line with the operations and autopoiesis of the system that allows it to maintain and reproduce itself.

System of IoT Development

The system of IoT development has not before been defined. As such, we need a binary distinction that will define the system itself. It can be argued that the system is a sub-system to a system of technological development or perhaps an even larger social system of technology. You could also argue for a social system of IoT that would include both users of IoT and academics writing about IoT. The working distinction for this thesis however, is: beneficial or detrimental for the development of IoT. This should be understood both in the literal and in the more abstract. For example, beneficial could mean a new technique to develop IoT or ignoring said technique if it risks triggering a response from the legal system.

Method

In order to observe the communication of the systems it was necessary to come up with a method that would reveal the communications. Luhmann himself did very little empirical research (Besio & Pronzini, 2008, p. 9) and it has been argued that it is hard to apply Luhmann to empirical research (ibid.). Besio and Pronzini (2008) argues that it is not only possible, but

that empirical research is structurally bound to systems theory because of Luhmanns emphasis of the role of theory and methods in science (Besio & Pronzini, 2008, p. 28).

There were a few ways in which this research could have been approached. One way would be a document analysis of the application forms and regulations regarding the applications for grants. Vinnova do have some ethical requirements in the application process (Vinnova, 2023). They are, however, somewhat vague. It would also only reveal how the developers argued for the ethics of their project in order to receive a grant. Whether the principles were actually held, or implemented would be difficult to discern. Because ethics are both principles and beliefs it is not only interesting to see how the ethics are implemented, but also how the people working on the projects view the beliefs. As such, interviews were selected as the most appropriate method. Since the focus of the thesis is on communication between different systems. Using semi-structured interviews would allow for a deeper insight into the thought process of the people working with IoT development in a way that quantitative methods would not allow. Semi-structured interviews were also deemed superior to both structured and unstructured interview for the purpose of the thesis. A semi-structured approach allowed for some pre-prepared questions to steer the conversation in the right direction. But, because the answers may provide further room for exploration, a fully structured approach would have been too restricting.

Any quantification of data would likely change the character of the study. One could imagine surveying the general attitudes amongst the people working in IoT. A survey approach would however likely miss out on a lot of nuances that are necessary to make the determination of how these ideas are communicated. As such, due to part of the aim being the individual views of managers in particular, interviews made for the best approach and would also give the highest density of quality data. As the focus was going to be on specific ethical principles and communication, some questions could naturally be prepared in advance using an interview guide (see appendix 1) (Bryman, 2016, p. 562). As such, semi-structured interviews were chosen as it would also allow for further exploration surrounding the questions depending on the given answers, further increasing the quality of the collected data.

Before the interviews the participants received a consent form (see appendix 2) and given time to read it ask questions and sign it. The participants were told in general of the purpose of the interview, while avoiding details that may have influenced any answers. The interviews were then conducted using the interview guide (see appendix 1) with some follow

up questions and sometimes requests for clarification. At the end of the interview all the participants got asked if there was anything further, they wanted to add. The interviews then concluded with a discussion where the subjects were told more about the purpose of the project. A back-and-forth discussion about the issues covered in the interview was then held which at times gave some further insight. At last, they got asked if they had any further questions about the project. After the interviews the interviews were transcribed using recordings from the meeting.

Sample

When choosing the subjects for the interviews, it was necessary to consider which interviewees would give the best insight into the operations of the system and specifically which interviewees would reflect the system the best with regard to the ethical principles. With regards to security, perhaps the security experts would have been useful. It is however possible that they would represent a different system entirely, perhaps a security system. Because the managers are the head of the projects and the decisionmakers, they were determined to represent the projects the best and have the best overview of the projects. As such, they would be at the center of the system and the most likely to reflect the system itself.

Due to the purpose and timeframe of this thesis, there were mainly two options available regarding sample. One option would be to use a snowball sample by finding a project or two and try to gain access to as many workers as possible within that or those projects. The other option was to use a selective sample to find as many projects as possible and as such widen the diversity of views as much of possible. Because Vinnova, the Swedish innovation authority has an initiative to fund IoT projects around the country, it was easy to find a diversity of projects in various areas of interest both geographic and with regards to focus. Because the focus is on ethical principles and both decisions and thoughts that goes into the decisions of the projects, managers seemed to be the best representatives of each project as they are the most likely to have the final say on these issues.

A decision was made to only focus on ongoing projects and not finished ones to ensure that these topics were as fresh in the mind as possible. As such the general sample size was quite small due to the relatively few ongoing projects in Sweden. In total nine people were contacted four women and six men from six different projects (some projects had more than one manager). Of the people asked all but one responded and as of now four have agreed to

interviews. Unfortunately, none of the women asked were, for various reasons, able to participate. Due to the reasons given, this appears to be coincidental. But will none the less be a weakness with the study. The tech-industry tend to be heavily male dominated, as such the effect this issue may have on generalizability may be a bit smaller than in other cases.

Out of the four interviewees three were made in person and one over Teams due to logistical reasons as the participant was currently situated abroad.

Interviews as Second Order Observation

Because this thesis is about observing the communication between systems, it is a second order observation (Luhmann, 1996, p. 258). Unlike a method such as document analysis, which is passively observing the first order observation, interviews are not just an observation. Through the interview an irritation is created within the system which forces the system to respond (Luhmann, 2013, p. 66). This comes with both advantages and disadvantages. An advantage is that, through the irritation created by the questions in the interview, the response is more likely to reveal the specific communications that are of interest. The questions can also be formed in way that will track the origin of the communication. For example, by asking whether the interviewee reads scientific articles or pay attention to the law, would indicate that the origin of the principle may be from those systems. One disadvantage is that the systems operations will always work to reproduce the system itself, meaning that the response of the system may be structured in a way that is meant to protect the system (Luhmann, 1991, p. 1419)As such, if the questions are viewed as negative for the systems operations the answers may be skewed to protect the system. Another disadvantage is that the interviewees themselves are likely part of several systems. As such, when asking about their beliefs it may be difficult to track which system the answer reflects. Just as with the systems, the interpretations are observations that are made with distinctions (Luhmann, 2013). The underlying distinction that is made is whether the answers indicate systems communication or whether they are individual reflections.

Design and Interpretation

As there are extremely few interview studies using Luhmann, and arguments about how to apply Luhmann to interviews are almost non-existent, it was not possible to find a framework for how to design the study. As a result, a lot of thought had to be put into the design. In an interview Álvaro Pires stated that intention needs to be treated as a *black box* when applying

Luhmann to an interview because you will not have enough information to argue for intentions (Pires & Sosoe, 2021, p. 21). He continues to add that the interview has to be viewed differently from how you would analyze documents, it is instead a way to understand communication using communication (ibid.). On a similar note, Besio and Pronzini (2008) argues that the researcher has to focus on communication and not attempt to detect the motives of indivudals as their intransparency would make it impossible (Besio & Pronzini, 2008, p. 22). Furthermore, they argue that interviews are communicative situations, as such the only thing that can be observed is communication. This based on a radical distinction between psychic and social systems where thoughts cannot be implied from statements, as whatever underlying thoughts may exist are bound by communicative rules and thus becomes communication (Besio & Pronzini, 2008, p. 23). To create a design within this framework makes it impossible to conduct interviews in a traditional sense where the focus is on thoughts and attitudes and interpretation of intentions (Bryman, 2016, p. 561). Instead, it was necessary to find a way to take a step back from the personal and look passed individual thoughts and attitudes and infer the systems communication. The solution was to take inspiration from the basic design of process tracing (Beach & Pedersen, 2019, p. 253). Within process tracing you can study causal mechanisms when a cause and an effect is known (ibid.). This is typically done in a temporal manner where one event follows another; the causal mechanism is then studied by finding empirical fingerprints between the two events (ibid.). Regarding the ethical principles the state of two out of the three systems are known. The legal system in the form of legislation and regulations and in the academic system in the form or scientific literature. As for the system of IoT development, questions were constructed to find the state. The communication thus would become similar to a causal mechanism where empirical fingerprints were needed to indicate that the communication had moved from one system to another. This is also compatible with Luhmann's views on causality, which is always contingent on the observer (Luhmann, 2012b, p. 92). The rest of the prepared questions where then formed evoke the necessary information for empirical fingerprints.

Unlike typical interview studies where the interviews are meant to study the views and the attitudes of the subjects interviewed (Bryman, 2016, p. 561), this study instead uses the interviews as a medium to get access to the systems communications that flow between systems. As a result, a heavier emphasis is put on the interpretation of the interviews. The questions for the interviews (see Appendix 1), as such, are structured for this very purpose. To access the communication several layers of interpretation are needed. Because systems theory is not about

communication and beliefs of individuals but instead about the communication of systems (Luhmann, 2013), a way to separate views held by the individual and reflections of the system is needed. As such, questions were designed to both ask about the views of the individual and how the teams had discussed the issues. Because the individuals are also part of the system, however, even the personal beliefs may be part of the system itself. Taking inspiration from thematic analysis (Beach & Pedersen, 2019, p. 235), answers given by different interviewees were also compared to each other to look for similarities this would also indicate a stronger empirical fingerprint. As similarities even in personal beliefs would indicate a reflection of the system. As a result, the data needs to be presented in a way that will have partial resemblance to a quantitative presentation where, the quantity of similar answers increases the quality of the data. Furthermore, there was a need for questions that could indicate whether communication between the relevant systems had occurred. The easiest way is to directly ask how much the interviewees had taken part of what was produced by the other systems. However, similarities between production in the academic system, the laws and the answers may also indicate communication. As such, there needed to be room for follow up questions.

Ethical considerations

Because the study consists of interviews and working with people, ethical considerations are necessary. First and foremost is the question of anonymity. Because the interviewees are project managers in their professional capacity working on projects with public funding and because anonymity was not of great concern for most of the interviewees, an argument could be made not to anonymize. However, due to the purpose of this thesis is aimed at communication of ethical principles between institutions, not to investigate whether people receiving public funding are following ethical principles, it was determined that very little would be lost by anonymizing. As such any names of participants, places and projects will not appear in the thesis and information that may allow tracking of participants will be avoided to the degree possible while maintaining the integrity of the project.

There is however the issue that the sample group of managers for Swedish IoT projects is rather small. As such, guaranteeing full anonymity is nearly impossible. This risk thus had to be considered before starting the research. Because the participants were not in a vulnerable position, are in a position of power, participate in their professional capacity, the research is not aimed at very sensitive topics, and an argument could be made not to anonymize, this was

determined to be an acceptable risk. Because of the risk however, all participants received written and verbal information explaining this risk before participating in the interview.

The second consideration was with regards to consent. All interviews need to be consensual, as such all participants received and signed a consent-form before the interviews with information about how recordings and data would be stored and handled, about the abovementioned risks, that participation was voluntary, and that consent can be withdrawn without reason given. They were also given contact information in case they wanted to withdraw or had any questions.

Generalizability

As the sample size for this thesis is very small and there is a clear lack of female representation in the sample it is hard to say that there is much room for generalization in this thesis. The reason for the small sample size is however due to the sample group being rather small. The technology sector is also largely male dominated. As such, while generalization may be difficult, the results should at least be useful as an indication for further research. As any similar studies have been done, there should be a lot of value even in a sample of the field to explore whether problems exist or not.

Methodological considerations

Niklas Luhmann is considered to be a radical constructivist. As such, using his theory as a theoretical framework also means that this thesis has to take the same epistemological approach. According to Luhmann, reality is far too complex to fully understand, as such any analysis of reality is contingent on the observer (Luhmann, 2012). Taking this epistemological position has both advantages and some limitations. Because any analysis is contingent on the observer, any observation of systems can only be done on the parts of the system within the environment of the observer. According to Luhmann the observer then makes his interpretation of the system based on the parts of the system he can observe and any causality within the system is then applied by the observer (Luhmann, 2012b, p. 92). The advantage of this perspective is that regardless of how much or little of the system you are able to observe, you can never observe all of it. As such any limitations such as the limitations here regarding gender becomes less of an issue. This, because the participants that are interviewed are always going to be the only part of the system available to the observer. Meaning, whether the interviews are

conducted with the subjects in this study or any number of other subjects regardless of identity of the subjects, it will always only reveal the specific part of the system that is observed at the time and regardless of the scope of the study, there is never going to be a study that can capture the full complexity of the system and is as such always contingent on whatever causalities are applied by the observer.

Naturally the backside of this is that it further limits the generalizability of the study, and any validity and reliability will always be contingent on the interpretations of the observer and are as such rather limited. It does however provide room for understanding of why certain answers are given and may not necessarily reflect the entire system. For example, as you can see in the analysis, regarding the answers to the questions about security. From the answers given there is an indication that the views on security are completely independent of the laws and the academy. The causality from the standpoint of the observer thus would indicate that the cause of the views on security comes from elsewhere. However, the respondents also indicated a low level of insight into the workings of the security systems and they typically left the development of the security to others. As a result, epistemological position inspired by Luhmann would then indicate that the causality is only a result of the position of the observer and a different observer with a better position for observing the security part of the system would possibly arrive at a different conclusion.

Validity and Reliability

Validity and reliability in qualitative research is not as straight forward as it is in quantitative research. One of the issues typically associated with interviews is the external reliability as the studies are often dependent on specific subjects for the results (Bryman, 2016, p. 456). The design of this study on the other hand, has the advantage of focusing on system communication rather than thoughts and attitudes of individuals. The focus on the systems means that the study can be replicated with any number of individuals from the system using the same questions, making the external reliability much stronger. It will however be an observation of a different part of the system and may give other conclusions due to the observer dependency (referems). But, even with different results it would aid in getting a more comprehensive view of the systems. Another advantage is that all the interviews were conducted by the same person making the internal reliability strong (Bryman, 2016, p. 456).

The internal validity of the study, in the sense that there is a strong connection between the theoretical ideas and the observations (ibid.), is both a strength and a weakness. The strength

lies in the entire study being conducted within a systems theory framework. On the other hand, the lack of previous applications of the theory to interview studies, may have a negative impact on the internal validity. However, adjusting the design using inspiration from established methods should act as a safeguard to this issue.

Previous research

This section serves two purposes, firstly to give an overview of the scientific literature. Secondly to also give an insight into the academic systems conceptualization of privacy, transparency and security in the context of IoT, to help indicate communication between the systems.

The literature review for this thesis had some challenges, because the number of papers written on the topic were both plentiful and lacking at the same time. While the first searches had an unmanageable number of hits and had to be restricted to the last three years to become manageable, the vast majority of papers were written from a technology perspective and addressed primarily privacy and security from a solution-based perspective.

To find the previous research search terms such as: *IoT*; *Internet of Things*; *Privacy*; *Transparency*; *Security*; *Ethics; Sociology of Law; Luhmann; Communication of Ethics* along with combinations of the various search terms were used. After selecting the top cited and most relevant papers, a noticeable lack of papers on transparency in IoT was detected. To account for this, more targeted searches were made and complimented with articles from the bibliography of the few results found. There were also very few papers connecting Luhmann to IoT, communication of ethics, IoT along with sociology of Law. As such, using the reference lists of the articles that were found, some of the gaps where filled.

Privacy and Security

The reason I put privacy and security under the same headline is because they are paired up in most articles. As mentioned in the background section, there are many issues regarding privacy and security when it comes to IoT. Starting with security the issue is that there are several attack-vectors from which you can approach IoT and all of them need to be addressed in order to properly protect the data (Mohamad Noor & Hassan, 2019). Each of the various layers of the IoT network are susceptible to attack and the ones using many devices are also risk various forms of attacks depending on the devices used (ibid.).

Of course, this also opens up privacy risks as the data then is susceptible to be stolen. Due to many devices being able to capture data in real-time but are lacking regarding data protocols and standards it is easy to collect and hard to secure sensitive data (Chanal & Kakkasageri, 2020). Also using private mobile devices as the sensory layer opens up further risks to the user regarding privacy (Jiang, Kantarci, Oktug, & Soyata, 2020). Alfandi et al. (2021) sums it up by saying that there are four basic security requirements of any IoT system: Integrity, Availability, Authentication and Confidentiality. Essentially securing the information from being modified or corrupted by malicious actors, making sure that the authorized people can access the data when needed, verifying identity of actors wanting access and making sure that private information can only be accessed by authorized parties (Alfandi, Khanji, Ahmad, & Khattak, A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues., 2021).

Proposed solutions

There are many proposed solutions to the issues regarding safety and privacy. The most common ones are Blockchain and Fog Computing (also called edge computing). Blockchain started off with bitcoin where it used a decentralized network of computers in a chain to secure the system (Alfandi, Khanji, Ahmad, & Khattak, A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues., 2021). Thus, it is a way to decentralize a network where data is spread on different devices using a digital ledger and an algorithm to organize the chain (Alfandi, Khanji, Ahmad, & Khattak, A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues., 2021). The decentralized nature of the blockchain is partially what gives it an increased security as any breach will only pick up part of the data thus blockchain is expected to revolutionize IoT (ibid.).

Fog computing or Edge computing is essentially cloud computing but taken down to the individual users and similar to blockchain decentralizes the process by partially using the devices of individual nodes to communicate on the “edge” of the network (Syed, Sierra-Sosa, Kumar, & Elmaghraby, 2021). Thus, similarly to blockchain it increases security through decentralization.

Both of these solutions however share a similar problem in that they require a very large amount of computing power and thus also consume a lot of energy (Syed, Sierra-Sosa, Kumar, & Elmaghraby, 2021). This makes it near impossible to apply to smaller IoT projects.

Transparency

Unlike privacy and security, there is far less literature on the topic of transparency in IoT. It is hard to say why this is, but it was clear from the interviews that the interviewees also had spent far less thought on the topic. Since the vast majority of the scientific literature surrounding IoT comes from the tech fields, in other words, similar fields as the IoT development, it is possible that transparency falls to the wayside as 'simple' or 'straight forward'. When in reality it is far from it. Most of the literature surrounding transparency and the IoT is focused on transparency regarding how, when, and what data is being collected (Nord, Koohang, & Paliszkiewicz, 2019). That is, if it is even argued at all.

Long et.al. (2023) identifies three issues with current strategies for transparency that are integral to the IoT. The connectivity between devices, users and the physical environment makes it difficult to notify how data is being collected and transferred between devices without logging into the system itself (Long, Luo, Zhu, Lee, & Wang, 2023, pp. 1-2). Secondly, the interoperability of the IoT and the way in which various devices communicate between each other and the physical space poses issues if one wants to track how data is being communicated (ibid.). Lastly, they argue that the development and integration of AI into the IoT and its increasing capabilities in data mining, causes issues in encryption and protection of data as well as data that was once thought to be non-personal to be pose a risk for identification (ibid.). They also explored the way transparency will affect how people perceive privacy and security risks and found that people transparency about who can access data, in what way the data is processed etc. will affect how people perceive an intrusion on their privacy. Furthermore, there are developing changes in the perception people have, where they found that people have a tendency to underestimate the capabilities of AI driven data collection and its capability of inferring personal information from seemingly far fewer sensitive data. It is however changing as people become more aware of how AI functions (Long, Luo, Zhu, Lee, & Wang, 2023, p. 8).

When thinking about transparency there are different ways of being transparent. The vast majority of articles about IoT and transparency is focusing on transparency in the collection of data, when data is being collected, how it is being collected and what form of data is being collected (Matheus, Janssen, & Maheshwari, 2020). There are however different ways in which one can be transparent which are just as important. Who will have access to the data? Under what terms is the data being sold? Who has a vested interest in the data being collected

including funding? What is the purpose of collecting the data? When it comes to tech there are some issues and difficulties regarding transparency. Especially how to maximize it. You could release all the data you have and hope that people understand it and can navigate it. But then you reach issues with privacy and data that needs to be detected. People often opt for a moderated form of transparency where you moderate the information you release in a more understandable way (Matheus, Janssen, & Maheshwari, 2020). There is also the issue of procedural transparency. When calibrating the measurements of the IoT devices and how it is collected, how exactly is it tuned? Brauneis & Goodman (2018) talks about so called "Type I Errors" and "Type II Errors" (Brauneis & Goodman, 2018, p. 120). Which corresponds to how an algorithm is tuned. A "Type I Error" is a false positive and a "Type II Error" a false negative, and algorithms will be tuned favor one or the other (ibid.). When treating sensitive data, there is a chance that the tuning of the algorithm behind the measurements may influence the conclusion. You can imagine it in the case of traffic cameras with sensors determining if someone is driving too fast or not. If it is tuned towards "Type I Errors" it will interpret an unclear measurement as a positive, meaning that driver will be photographed and possibly receive a ticket. If it is tuned to favor "Type II Errors" it will only take a photograph of a driver that is clearly in the wrong and any unclear measurement would be ignored. Transparency in this case would be to tell the drivers whether or not they risk a traffic ticket when they are driving exactly at the speed limit. It is not hard to imagine people becoming rather upset in the case of a "Type I Error".

Luhmann and Sociology of Law

Luhman wrote surprisingly little on the topic of technology. When talking about security and technology he refers to social security rather than security in the technology (Luhmann, 1990). He took issue with the concept of security arguing that it is simply a counter-concept to risk (Luhmann, 1990, p. 225). Arguing that it should instead be viewed as a distinction between risk, as the introduction of new technology is meant to alleviate one risk but will inevitably come with its own risks (ibid. 226). The prevalence of IoT is of course after Luhmann's time, but even among others the literature review revealed no relevant peer-reviewed articles pertaining to Luhmann and IoT. On ethics Luhmann primarily arguing surrounding the role of ethics in society and issues surrounding its implementation and how sociology should tackle ethics, rather than the communication of ethics between systems (Luhmann, 1996). In the same article however, he argues that ethics are realized as

communication but leaves it to future sociologists to figure out (ibid. 32). Just as with IoT however, relevant peer-review articles on systems communication of ethics are hard to find.

In sociology of law IoT is also scarcely researched. Håkan Hydén (2023) briefly mentions the risks to privacy and security of IoT in an article primarily focusing on AI and algorithms, emphasizing the issues of IoT devices entering private homes (Hydén, 2020, p. 358). As such, there is a very large gap in the scientific literature both with regards to Luhmann, ethics and IoT, as well as within the literature of sociology of law.

Laws and Guidelines

To be able to understand how the ethical principles may be communicated between the legal system and the system of IoT development, it is necessary to get an overview of how the legal system approaches these principles. As such, here is a brief summary of the relevant legislation and how it applies to the principles at hand.

General Data Protection Regulations (GDPR)

GDPR is the EU's comprehensive regulations regarding the collection of people's personal data. As it pertains to IoT GDPR regulates that organizations need to have a legal basis for how they process personal data. For example, requiring user consent for data collection and processing (Article 6). It also emphasizes transparency, and information meaning that users must be informed of how and that the data is being collected and how it will be used (Article 5). Furthermore, organizations need to minimize the data they collect and not collect any data that is not essential for the stated purpose (Article 5). GDPR then requires that this data is being stored securely to protect any sensitive personal data to leak to unauthorized parties (Article 5). It also protects the rights of users with regard to their personal data such as access to it and the right to have personal data erased (Article 17). In addition to these things GDPR also puts requirements on Data Protection Impact Assessments (DPIAs) which is applicable on large scale projects with a lot of sensitive data, as well as how data can be transferred outside of the EU and regulations regarding accountability of organizations (Article 35).

In terms of our ethical principles, privacy is the overarching theme of GDPR and both transparency and security ties into it. The transparency becomes very important with regards

to both user consent and the rights of the users. Since you need to be aware of the data existing in the first place to be able to request access to the data or that the data should be erased. Similarly, security becomes essential as part of GDPR to make sure that the privacy of users is protected from unauthorizes actors by protecting whatever data is collected.

Enforcement of the GDPR is left up to each EU member state, where each state has a designated Data Protection Authority (DPA) that acts as supervisory authorities. Their responsibilities are to monitor, investigate, audit and issue fines for violations (Article 58). If an organization is in violation of the GDPR complaints can be sent to the DPAs and they can do an investigation of the complaints (Article 58). They can also have the power to conduct inspections or audits regarding how data is processed by various organizations (Article 58). If the organizations are found to be in violation of the GDPR they can issue large fines (Article 58) Additionally corrective measures can be issued to organizations for the purpose of rectifying any violations (Article 58). Because organizations often span several states DPAs also cooperate across borders facilitated by The European Data Protection Board (EDPB).

Because the GDPR is enforced locally within the member states there may be some variations of how it is interpreted between states and to what degree it is being enforced. The DPA in Sweden is the Swedish Authority for Privacy Protection (Integritetskyddsmyndigheten)(IMY). They are also in charge of the enforcement of Sweden's Camera Surveillance Act (Kamerabevakningslagen) among other responsibilities (SFS 2007:975).

Sweden's Camera Surveillance Act (Kamerabevakningslagen)

Another law that came up in the interviews was Sweden's Camera Surveillance Act, which regulates how and when you are allowed to put up surveillance cameras and how to handle the recording data (Kamerabevakningslag (2018:1200)). As such it has certain overlaps with the GDPR. The act requires that private companies, public authorities and individuals need to get authorization from the Swedish GPA if they want to put up surveillance cameras (ibid.). It also requires that the cameras need a legitimate purpose for surveillance, such as public safety, crime prevention or property protection (ibid.). Furthermore, individuals must be informed when they are being surveilled (ibid.) and the surveillance need to be necessary as well as proportionate for the purpose of the cameras (ibid.).

Results

As previously mentioned in the method section, unlike typical interview studies where the purpose is often to get an insight into a person's thoughts and beliefs, this study instead focuses on answers given as indications of system communication. As such, the presentation of the results will also differ. Borrowing the terminology from process tracing the results will be presented with indications of empirical footprints (Beach & Pedersen, 2019, p. 253). However, unlike process-tracing these footprints are not indicating a causal process (ibid.), but rather indicating communication or lack of communication. Also as was stated in the method section, part of the interpretation of the data is to separate individual beliefs from system beliefs. As such, agreement between respondents can be interpreted as a stronger empirical footprint. Thus, some of the data will be presented in a more quantitative manner to help with this analysis. It will also be complemented with some direct quotes that can help contextualize some of the answers or give indications of missing communication.

Some information has been redacted from the quotes, mainly to protect the anonymity of the interviewees. That is information such as names, places, individual organizations. Since the number of IoT projects in Sweden are limited, detailed information about the projects could also very easily lead to identification. As such, the details have been kept to a minimum and any details that are not necessary for the analysis have also been redacted or made a bit vaguer than were first stated to protect the identity of the subjects. The questions for the interviews can be found in the interview guide (see appendix 1). Because the interviews were semi-structured, follow up questions were sometimes asked and some of the questions may have been skipped if the answer had already been given to keep a better flow of conversation. Rather than presenting each interview individually, the results will be presented under a topic, to help search for empirical footprints, it also further protects the identity of the interviewees.

All of the interviews were conducted in Swedish. All quotes have been translated from Swedish to English.

Interviewees

Here the interviewees will and their projects will be very briefly presented. The information here needs to be very minimalistic due to the small group of individuals the sample is taken from. All of the names of the interviewees have been changed to ensure anonymity. Some of the details may also have been changed for the same purpose.

Victor

Victor was working on a very small project directed towards healthcare. With a background in the academy directed towards engineering and the interaction between technology and its interaction with people. The project was the smallest.

Dennis

Dennis was working on a project measuring traffic. The project was part of a much larger initiative with several other projects which he was also in charge of. He had years of experience in various projects related to IoT.

Robert

Robert was in charge of a project directed towards outdoors activities and was meant to be part of a full smart-city development. It was the largest project. He had decades of experience in IT and project management.

Mark

Mark was leading a project directed towards indoor environments. At the time of the interview the project was at a very early stage. It was the second smallest project. He had background in the tech sector and as a project manager.

Privacy

An interesting aspect surrounding privacy that came to light during the interviews is that the perspective on privacy differed a bit with the nature of the project. Victor's project had to do with healthcare. As such, privacy was one of the first priorities and the project was able to use the expertise of nurses cooperating on the project regarding the topic of GDPR and privacy. While Mark had made decisions early to avoid certain technologies so that they would not have to worry too much about ethical issues. When asked how they had discussed these topics he said:

> *"We discussed things such as integrity early in the project. You start off with a large collection of possibilities that you discuss. Such as, well, there are cameras. Absolutely, there are cameras, but then you get into the problems of integrity. Who has access to them? What is the data going to be used for? Such things. So, we completely went away from cameras and instead opted for very passive instruments, that just give you a value of measurement."*

This is a strong empirical footprint indicating a structural coupling between the system of IoT development and the legal system. It indicates an anticipation of a response from the legal system causing the system to adjust its operations before the response was triggered (Luhmann, 1991, p. 1424).

> Because Dennis was manager for a larger initiative in which the project was a part of. He was able to use the experience from previous projects and help from a lawyer hired for the larger project to get more insight into how the legislation was to be viewed.

The participants were also asked whether their project was meant to be connected into a larger context, such as a larger project or perhaps into a smart city system. One was not, one was part of a larger project, and one was meant to be part of smart city development. This was later reflected in the question of whether they had given any thoughts surrounding these ethical issues for the future when the collected data could be part of a much larger data set.

When asked about his thoughts about data being collected and then aggregated Dennis said:

> *"The most important concern is when you get this large pool of data such as with IoT when you collect for a platform. Ours is built more like a greenhouse where you collect data and then send it off to a larger system. But in cases where you have everything collected and you can start combining it and draw conclusions about people act. Then… those things are super important, that you really know what you are doing and what is happening. In our system we have the capability to separate more sensitive data from the rest so you can remove data that you cannot make public. Our intention is to, as much as possible, publicize as open data. But we have had situations where we are working with sensitive data. Then it is not possible."*

Robert stated that this was a concern at every step in the project and that they had to be constantly aware that even data collected without any capacity for personal identification, could when corroborated with a greater set of data become a privacy issue. He had the following to say when asked if they had discussed ethical implications when data is aggregated:

> *"Of course! In these cases, you need even better planning and better thought behind how you present, and what data you present. You never want 'sit there with the beard in the mailbox' (Swedish saying, closest English comparison is probably 'deer in the headlight') and be surprised or 'get caught on the bed' (another Swedish saying, similar to 'caught with your pants down') with someone saying, do you not realize that you can get such and such information. Cross reference or aggregate the information. The more information you get, the more useful it is but you must think about it even more, including regarding safety."*

Mark whose project that was not immediately meant for a larger project had a different perspective regarding risks of aggregated data. When asked about whether they were thinking about how the data could be used if aggregated with other data he said the following:

> *"If it is not personal data, but instead general data that is being collected. If we are satisfied in general within the team, then I do not see any major risk about it. But it is a question of which type of data that is being sent."*

He was asked to clarify whether he meant that if the data is not personal on a small scale, then it should not be a problem on a major scale. He said that it was mostly about how the person experience the measuring, if they think it is a problem or not.

This problem is discussed a lot in the academic literature, as such the reflections of the viewpoint in the larger projects makes for a fairly week empirical footprint. However, it does indicate that the system will primarily reference the internal binary (Luhmann, 1991, p. 1427). When the projects grow large enough that it may trigger a detrimental effect to ignore the communication from the academic system, the system will start to integrate the communication.

When asked about the participants own thoughts on privacy and where they thought the line was on how much invasion into privacy is acceptable the answers varied to some degree. One participant was much in line with the legislation and thought that collection of data should be okay as long as identification of individuals or specific groups is not possible.

When asked where he thought the line should concerning integrity Robert stated:

> *"I think the line should be drawn where you can tell that I am the one doing something. That I have acted, and you can see that I am the one that has done something. Or when you have a group that does something, for example when you have a group whose age is such and such. Such a group cannot become too small, so you can start identifying individuals within the group. That is where I think the line is, when you can intrude on the personal integrity or the group integrity. Also, when you have things such as race or sexual orientation and things like that. If it is more general such as you can see for example that I have moved from point A to B or that I have used something. But, if you have to pay for example and you can start seeing the payment information, then you start getting into problems."*

Victor took a more utilitarian approach in that collection of personal data should be subject to a cost/benefit analysis, meaning that any collection of personal data should have to be justifiable regarding the benefit of collecting the data. He said:

"When talking about integrity in healthcare, you always ask the question: 'will crossing a certain line benefit the patient?'. Some of the ways we record data are intruding on the privacy of the individual in some ways, but is it worth it? Will it benefit the patient? Because there is no reason to record the data if there is not any value in it. You have to determine the potential value in what you are doing. It is the same in the agreements that we have signed. You have to motivate what you are doing and how you process the data. If your only motivation is 'it would be fun', that does not work, then there is no reason to implement it."

Mark had similar thoughts when asked about his personal beliefs on where the limits on privacy intrusion should be drawn. He said:

"It is a very difficult question. In my world, it is dependent on the purpose, and what you are aiming to use the data for. At the same time, I can understand another perspective, that you do not want 'Big brother' looking over your shoulder at all times. It is difficult as I said. It is very difficult. I am both for and against using personal data. It depends on the purpose and whether the purpose can be maintained."

While there is a discrepancy of the answers, they are mostly in line with the GDPR which states takes the purpose of the collection into account and draws the line at personal or group identification indicating an empirical footprint.

Transparency

Regarding transparency, most of the participants had not given it much thought outside of making information about the projects available as they were developed.

Dennis explained their strategy for transparency:

"We try to be as clear as possible to the outside about what we are doing in all of our projects. For example, we have our website, were we put up information about the projects, about what we are doing and how we are doing it along with contact information. Where we have been able to respond to any questions and concerns from the public. It is much easier to do the project if you are transparent about the project, about what you do and why you are doing it. Then there are very few questions from people. Of course, in some projects we have received some comments from the public where people do not want us to put up sensors at all but being clear on the website and through social media etc. drastically reduces the number of complaints."

Robert however, had given it some thought and was aiming to put up signs where data is recorded to notify the public of how and when they are recorded. He did however admit that transparency had fallen to the wayside and that they had not been as transparent as they should. Saying when asked about transparency:

> *"On that topic we could and should have done more. We could have put up more information surrounding it. It has unfortunately… it became unfortunately a shortcoming, because the communicator that we were supposed to have, was moved to a different project. But we have still been able to do some things. Where we have sensors, we have been able to put up some signs saying what is going on and tell people that what they are doing is being measured but not that 'you' are doing it."*

Most of the participants did not have a clear thought on just what it meant to be transparent. One even had to ask what I meant by transparency. Similarly, to most of the literature surrounding transparency, little thought had been put into different forms of transparency, such as funding, who will have access to data and so on. Rather, comments mostly surrounded information about when data will be recorded and by whom. As the GDPR puts heavy emphasis on transparency (Article 5), and transparency is also explored in the academic literature, this is a strong empirical footprint indicating a lack of communication of transparency from both the legal and the academic systems.

Robert had an interesting answer when asked what transparency looked like to him. The project was directed towards outdoor environments and activities measuring availabilities of tools and places for activities and environmental data such as weather conditions. The data collected is meant to be available in an app where people can make us of it. When asked what transparency was, he talked about the future of the project and the app essentially making the information available so that people will be able to make as much use of the service as possible. Meaning that the answer became directed towards giving as good of a service as possible, rather than towards the concerns about transparency which is the primary focus in the law and in academia. Another respondent gave a very similar answer, talking about the improvements that the IoT will make to the people using it and how much more they would be able to do with the information. Important to note is that these two projects were directed to measuring environmental data or data on things rather than people. As such they had probably the least number of sensitive measurements of the projects. This empirical footprint is indicating that the topic of transparency is only understood on the basis of the internal binary communication

of beneficial or detrimental to the system and is thus presented through reference to the operations of the system as it is the only way it is understood (Luhmann, 1991).

Mark's projects focused on environmental data within buildings. Because it will not directly record data on people, little to no thoughts had been put towards transparency. Again, the answer is indicating self-reference and a footprint indicating missing communication between systems.

Victor added at the end of the interview some reflections about transparency when asked if there was anything he wanted to add:

> *"I was thinking about transparency, it must be very difficult when it comes to IoT, since it is often meant to be invisible. The solution in our project is not very invisible since it puts it right in your face. But I was thinking, other solutions must be very difficult to be transparent with. I was thinking some of the other projects in IoT-Sweden are about measuring things such as various flows, or when you put up sensors. It must be very difficult to be transparent."*

This is an empirical footprint indicating that there may be an incompatibility with the internal operations of the system of IoT development where negatives of being transparent outweigh the positive, moving the interpretation of transparency in the internal binary from beneficial to detrimental.

Of note regarding the answers on transparency. The way in which the projects had attempted to be transparent exclusively fell in the domain of moderated transparency where they would collect information which they would put out on a website, in an app, in a message when the application was used or on social media. Different forms of transparency which were mentioned in the section on previous research were not mentioned at all. No one mentioned how the measurements were tuned whether it was towards "Type I Errors" or "Type II Errors" or transparency regarding the algorithms behind the technology.

Security

As it pertains to security, all of the participants stated that they had taken security measures and discussed security issues with their teams, they did not however go into detail as to which measures had been taken and how they would ensure security.

Dennis stated:

"I am no expert on security, so I do not know exactly which protocols we are using. But there are certain safety protocols that are in place to make sure that the data is protected and to prevent unauthorized people to access the data. This IoT platform also has a safety trigger that prevents people from looking at the data where it is being collected. However exactly how it works, I do not know"

Some gave indications towards encryption of the data and using existing programs for encryption but nothing in detail. It is possible that the participants wanted to avoid going into security in detail since publicizing security details may compromise the security itself. Victor however said:

"We have discussed security and it has mainly been about preventing people from accessing our solution and it has a safety classification on some very high level. Since we are not saving any data we do not really have to worry about access to the data."

Mark simply said that they have safety as a concern but that they are leaving it to their IT-department and that they have complete faith in that they know what they are doing.

Unfortunately, the part of the system that was observable using the interviews, largely did not include the security measures that were taken, as such it is difficult to indicate any empirical footprints based on the answers given.

Security measures proposed in the literature such as blockchain or fog computing was not mentioned by any of the participants. Due to the scope of the projects, it is however likely that none of them were nearly large enough to justify the infrastructure needed to justify such measures which becomes an empirical footprint indicating a lack of communication between the two systems, as the proposed solution becomes incompatible with the part of the system that was observed.

Considerations

All of the participants were asked as to what they took consideration of when they discussed the ethical issues at hand. All of them responded that they looked towards the law and guidelines such as GDPR. Victor said that working alongside doctors who deal with sensitive data and an adherence to GDPR on a daily basis gave additional insight into how he should consider GDPR. Robert stated that conferences with other IoT developers were very useful for learning how to adhere to the regulations and how others are interpreting it. Dennis expressed some frustrations with the localized enforcement of GDPR and said that there was a large discrepancy between states with regard to how GDPR is interpreted and enforced, with

Sweden being the strictest. He said that other states views GDPR more as guidelines rather than law.

Talking about Sweden's Camera Surveillance Act:

> *"…the law is written in a way where if you yourself is standing with a camera in your hand, then you are allowed to record data. Meaning, if you have your hand on it and stand there looking yourself, then you can record … it is very very strange in a way. I understand why the law is written the way that it is. But at the same time, it is very difficult for Sweden to be at the forefront, because there is no exception regarding innovation."*

He expressed a frustration with the logic behind the law and a lack of flexibility with the way the law was constructed. He then continued:

> *"There is a possibility to apply for permission if you want to put up cameras, if you put up signs and restrict the area. The issue is, if you want to apply for permission there is a 12-month waiting period just to get it through, and then you do not know whether you will get it or not. It is very difficult to do in a publicly funded project when you have a time limit. As a result, since we have experience working with this, it has been very difficult to get it through. In Stockholm they have really run into issues surrounding this. So, we have had to limit what we collect."*

When asked about whether the laws and regulations are good the way they are or whether some improvements were needed and whether the more, or less regulations are needed:

> *"I think that some practical examples may be needed, of best praxis cases for example, the various institutions that exist for the Swedish municipalities should be able to be more proactive with best praxis for us municipalities. We are 290 municipalities and with that many it is very likely that we are in violation in many cases. But I think it has more to do with a lack of knowledge or that lack of understanding of the broader context … Also, I mean, you could possibly simplify it. But at the same time, it is a protection that is needed for the individual. Because it would be very unfortunate if it did not exist."*

When asked to clarify he said that the laws themselves are about what they should be but that we may need some more guidelines. He then continued saying that, sometimes not even the lawyers may be able to know exactly how you are supposed to interpret the laws. Especially he emphasized an issue with how the EU regulations are written. Another respondent had a similar answer when asked if the regulations were good or needed some change saying:

> *"I think GDPR gives pretty good guidance. It is a question about integrity, it does bring up security as well, actually. Is it anything more I would like from the legislation? The problem is you need a lawyer to help you. Otherwise, you are just guessing. You can get*

some understanding from just looking at the law, but eventually you need a lawyer that can tell you if you understand it correctly, which is a shame."

He later also stated that the some of the guidelines from the EU that are meant to help people navigate the laws are helpful, at least to a degree. I said that they helped in the beginning to put you on the right track and reduces the need for a lawyer, which is helpful due to how expensive lawyers are. He emphasized that you still need a lawyer but that you can at least bring what you have learned from the guidelines when you first meet the lawyer.

When asked whether they had read any of the scientific literature on the topic, all but Robert said no. Robert stated:

"We read to the degree that we have time for … the projects are built to be a prototype and there are questions of how you are supposed to man them and how to manage everything. Ideally, perhaps every project should have a lawyer as part of it for example."

In essence he stated that ideally one would have experts on hand to cover all the basis, but due to limitations with time, resources, and manpower, it is inevitable that you end up falling short at times.

Victor was an academic himself and said that they had had other academics as part of the project but had not directly discussed what the academy had to say. He however stated:

"If you are talking to product owners at a company, along with people working for the region and yourself, it is not like you talk in an academic way, even if you are an academic. It is not like you are referencing academic articles, even though that may be where your knowledge comes from. But given the areas of the other academic part of the project I can imagine they have extensive knowledge about integrity, and I do have some myself. But, we are not talking academic concepts when we meet"

The participants were also asked if they got to study ethics in school (all of them had some form of tech-related education), the older ones that had studied 15 or more years ago said no, but that they had noticed that the younger people coming along had more education on these topics. Victor, the youngest, participant said that he received quite a lot of ethics in his education but that it was most likely due to the nature of the education. When asked about how much he got to study he said:

"Quite a lot actually, I have an engineering degree. But, my education was about putting the human at the center, so it was directed towards the needs of people. As such it was a bit of a mix between psychology, engineering and design. So these topics were quite central. It was definitely more than a normal technological education. Because the focus

was on the human not on the technology. Most engineering educations have its focus on the technology."

The empirical footprint that can be interpreted from this section is that communication is indicated from the legal system. Even with the complaints about the formulation of the laws it still indicates that the system is receiving the communication. At the same time, the complaints are also indicating a difficulty in translating the communication into the binary distinctions of the system of IoT development. The Academic system on the other hand does not give any clear empirical footprints that indicate a proper communication. Since Victor was also part of the academic system, whatever academic texts he was reading, would reflect the academic system rather than the system of IoT development. However, what he learned from his education would indicate an improvement from the academic system to communicate using education rather than through academic texts.

Analysis

Whenever the system of IoT development reacts to an utterance it will always do it with reference to its own binary distinction of beneficial or detrimental to the development of IoT. This is entirely in line with the autopoietic nature of systems (Luhmann, 2013). This is reflected in the discrepancy of how projects at time differ in their reflection of the values in the other two systems. For example, when a project is meant to be part of a larger context, whether the considerations addressed in the scientific literature were reflected or not were dependent on the intention for the project. Where the ones that were meant for a greater context would reflect the academic system and the ones that did not, would not. Whether this indicates a communication from the academic system remains to be explored. However, it does indicate that, when there is a risk of triggering a response from a different system, whether it is the legal system or some other system the considerations moves from beneficial to detrimental for the specific operation in charge of the project. Due to the potential future impact of the project on other systems, it must have a structural coupling to another system that it anticipates will have a greater detrimental effect on the operations than the cost of the concern. This also reflects the way Luhmann addressed technology and risk (Luhmann, 1990, pp. 225-226). The system of IoT development need to make a distinction between the risk related to the benefit/detriment of the different approaches (ibid.).

Due to the nature of the IoT itself and its applicability and malleability to various sectors, the various projects of the system of IoT development will naturally have very different

environments from each other. When the project is targeted towards healthcare, it is able to observe the healthcare system and integrate its views on the laws and the ethical principles, taking inspiration from doctors. At the same time, projects directed more towards non-human data will have far less information about the ethical principles within its environment and thus will become more self-referential. It appears a lot of the thoughts on privacy comes from a more common sense understanding of it. Perhaps individuals working within the development thinking to themselves, what they would view as an invasion of privacy. As such, the nature of the project will heavily affect how much ethics is considered. It also appears that the projects within the system of IoT development learn from each other though conferences and meetings with other projects. As such, the system replicates itself through self-reference when the subsystems observe each other.

Communication with Law

From the results of the interviews, it became quite clear that the legal system has the capability to create significant irritations within the environment system of IoT development, large enough that the system has to respond to it (Luhmann, 2013, p. 88). From the result we can conclude that there is a structural coupling between the two systems. All of the projects had at least looked at the GDPR early on in the project. Mark even stated that they had moved away from using cameras almost immediately to avoid any problems with GDPR. As such, we can infer a structural coupling that caused an anticipation of how the legal system would respond to the implementation of the cameras, as such when the system reproduced itself it adjusted its operations to exclude the use of cameras (Luhmann, 1991). The risk of triggering a response from the legal system was determined to outweigh the benefit of using cameras. As such, using the language of the system it determined that the use of cameras would be detrimental to the development of IoT and avoiding it would instead be beneficial. When the system then reproduced itself without cameras, it positioned the operations in a way where the GDPR would no longer be able to make irritations in its environment. As a result, however, since they did not collect personal data and was not planning for any big data situation. When asked whether they saw any risks with aggregated data they had the same views as on a small scale, that as long as the data is not personal on a small scale it should not be a problem on a large scale either. Aggregated with other data it is possible that the data eventually become personal, and GDPR reenters the environment. Which is something Robert's project directed towards outdoor environment but was planned for a smart city was very aware of. Since GDPR only states what personal data is, not really at what point non-personal data can become

personal data, the anticipation created by the structural coupling caused him to be much more aware of the risks associated with aggregated data.

There does however seem to be an issue with the translation of the communication from one binary to the next. As was expressed by Dennis, the way that the camera surveillance law is structured and the lengthy process of application along with a seeming arbitrariness to when a camera is permissible and when it is not, causes issues in the translations. It becomes very difficult for the system of IoT development to properly integrate the law into its own binary. Cameras become extremely difficult to use as a result.

Privacy

When asking the participants about the legal system, privacy and integrity was always the first thing that came to mind, especially in the context of GDPR. All the projects had considered GDPR and privacy to some degree, two had included lawyers. This indicates that on the topic of privacy the legal system is able to communicate with the system of IoT rather well. The question is the reason for it. It could be that the legal system is stricter on privacy and any violations are easier to detect than are violation of other parts of the GDPR and as such the irritation within the environment of the system is greatest with regards to privacy. Of note however, when the participants were asked about their personal views on privacy and integrity, their responses were largely in line with the GDPR. Saying that privacy becomes an issue when it is personal data and that you need to justify any intrusions on privacy with the purpose and benefit of the project. What this indicates is that rather than the legal system communicating how to value privacy, the values are already in the system. When the irritation is created in the environment the self-referential observation of the irritation allows the system to integrate it into itself without having to make any changes when reproducing itself.

It seems to differ somewhat when it comes to the camera surveillance act. It was only mentioned by one of the subjects as he was the only one whose project would greatly benefit from surveillance cameras. His comments on the act and adherence to it were however rather negative and indicated a frustration with it. In this case the legal system was not necessarily corresponding with the values already within the system. Rather the risk of enforcement meant likely created enough of an irritation to force the system to adapt. When others had discussed cameras, they had mainly done it within the context of GDPR and opted not to do it. The question is why this phenomenon appeared. Why the first inclination was to look towards the GDPR rather than the camera surveillance act, and why the camera surveillance act was

considered against some internal values of the system. The reason is likely to be that the GDPR is far more well known amongst the general public. As such, it is likely top of mind when thinking about data collection and privacy, especially since it covers far more relevant areas as well. As a result, it exists within the environment of the system from the very start. If the system disregards using cameras because of GDPR, the camera surveillance act will never enter its environment. If, however, cameras are further considered, the act will enter the environment. Because the camera surveillance act is a Swedish law with Swedish enforcement, and it also demands that you apply for permission, its enforcement capabilities are much stronger. As such, by the time it enters the environment of the system, it creates a far stronger irritation and can force the system to adapt even if it is not in full agreement.

Security

When asked about laws and regulation, security never really came up. When asked about security GDPR was mentioned once but just as an afterthought. Security was however a deep concern in all the projects. The concern just did not appear to come from the legal system but from somewhere else. None of the interviewees were in charge of security and did not seem to have deep insight into how security was implemented in the project. As such, because this thesis is a second order observation, whatever conclusions are drawn can only be drawn based on what is observable by the observer. It is thus possible that the parts of the system that communicates with the legal system regarding security, was outside of the environment of the observer (the interviewer). The causality that can be interpreted from the interviews is that the legal system did not cause the values about security to the system of IoT development, rather they must have come from somewhere else. But, with the caveat that the causality is contingent on what is observable by the observer (Luhmann, 2012b, p. 92).

Transparency

The communication of transparency is a rather interesting case. The GDPR heavily emphasizers transparency. But it was never mentioned by the interviewees when asked about GDPR and GDPR was never mentioned when asked about transparency. Rather, transparency was mostly treated as an afterthought. Also, GDPR treats transparency as integral to its privacy protections and because it requires that people should be in control of their personal data and know when it is being collected. As the respondents' views on privacy corresponded quite well with the GDPR but you find such a discrepancy regarding transparency is thus interesting. It would further indicate that the integration of the GDPR's values on privacy did not come from

an irritation created by risk of enforcement, but through some correspondence with the self-reference of the system. As such, if the system does not carry the values of the GDPR regarding transparency, it becomes difficult for the legal system to create enough irritation to force a response by the system of IoT development.

This calls into question the actual capabilities of the legal system to communicate with the system of IoT development. The thoughts from one interviewee where he stated that transparency would likely be an issue with other projects, because IoT detection is often meant to be invisible may provide some insight. The GDPR is written to be very broad and apply to many different areas. It was not written specifically with IoT in mind. Several of the interviewees expressed troubles in interpreting the GDPR and knowing exactly how it should apply. An issue one stated even lawyers had. As a result, when the technology is meant to be invisible and the laws may or may not be applicable to the situation, it may be difficult to know how to apply it. Since the system can only observe through self-reference and determine whether what it observe is applicable to its operations, the system may simply not be able to properly observe the GDPR's views on transparency as it does not know how to integrate them into something meant to be invisible. A solution may be as some of the interviewees mentioned, to create a best praxis or guidelines specific to IoT to help understand how they should navigate the law. It may make the communication with the system easier as it can create irritations that corresponds better to the systems operations.

Communication with academia

The communication between the academic system and the system of IoT development appears to be even weaker than that of the legal system. There are likely several reasons for this. For example, the academic system does not have the enforcement capabilities of the legal system. As such, the irritations it creates in the environment are not nearly as strong. The academic system has two main methods of communication, academic writings such as books, articles in journals etc. The second is education, by educating students it can communicate with whatever system the students enter after graduating. Academic writings have a few problems of reaching the system of IoT development. The first problem is *financial*. You have to buy books and papers are often hidden behind the paywall of academic journals. As such, you must pay to receive the communication. The second problem is *time*. The output of academic writings is so vast, that in order to keep up, you have to spend a significant amount of your time just reading. Which is something the one interviewee, who said he read some, stated as a

problem. Since the developers have to spend their time working on the projects, it is unlikely they will have time left to read unless they find it very interesting. The third issue is *reach*. Unlike the legal system, which will come knocking on your door if you do not pay attention to it, academic writings for the most part are just released. You will have to look them up if you want to know what they say. As such, their ability to create irritations are very limited.

Concerning the binary distinction of the academic system of academic or non-academic knowledge where academic knowledge was defined by its marketability to publishers, journals and students. There remains a question as to whether communicating these ideas to the system of IoT development is actually compatible with its operations, at least in the context of academic writings. While at first glance, the academic system is very inclined to solve the system of IoT development's issues regarding the ethical principles, due to a lot of solutions being proposed. Implementation of workable solutions would actually reduce the academic systems capacity to reproduce itself. The larger the issues are in the system of IoT development, the higher the demand for the production of the academic system will be. From the results this is reflected in the solutions proposed by the academic system. By far the most common suggestion for privacy and security concerns was the implementation of blockchain technology (Alfandi, Khanji, Ahmad, & Khattak, 2021). However, due to the high monetary and energy cost of said solution, very few IoT projects are actually large enough that it would fall under the beneficial in the binary distinction. As such, it is unlikely to solve much at all. What it does however, is creating further opportunity for production within the academic system, where new academic papers can be produced about challenges with blockchain (Liang & Ji, 2022) or improvement to it (Wazid, Das, Shetty, & Jo, 2020).

The second form of communication from the academic system, education, has some advantages and some other issues. The advantage of communicating through education is that hiring people with university degrees is already a part of the system of IoT's operations. As such, the system of IoT development already has a strong structural coupling to that part of the academic system. As a result, if the academic system teaches the students its views on the ethical principles, they will be communicated through already established communicative lines and does not need to create new irritations in the environment. Instead, it immediately becomes part of the self-reproduction of the system of IoT development (Luhmann, 2013). It also has the advantage that the solution is in line with the internal binary of the system. Unlike the production of academic literature, the marketability of the solutions communicated through the students are actually beneficial to the operations of the system. Because it makes the students

more attractive to the on the labor market increasing the marketability of the academic knowledge. The downside of education is its speed of communication. It is a very slow form of communication. Integrating it into the curriculum will not have an effect until after the students graduate. Furthermore, when the student is hired, you still only have one member of the project that carries the knowledge. Not to mention, it is likely the youngest member with the least authority. Furthermore, it is not guaranteed that these principles will be what the student brings with him from the education.

From the answers given, there seems to be some usefulness to education at least. While the older interviewees did not learn much about ethics in their education, they did state that they younger members of the projects had brought some ethics with them from the university. Indicating that the education form of communication has some impact. One of the interviewees also mentioned that he was part of the academy and that other academics had also been part of the project. As such, there seems to be a structural coupling between the systems where the same people may be part of both systems simultaneously and will be influenced by the academic system in their thoughts on the topics.

Self-reference

According to Luhmann, there is no difference between self-reference and observation, and all communication is observation through self-reference (Luhmann, 2013). Furthermore, communication can also happen within systems, not just between them (ibid.). The question then becomes, how much are these ethical principles communicated from other systems and how much is simply self-reproduction through self-reference? It is impossible to determine exactly, but there are some indications in the answers given by the interviewees. Robert mentioned that he would learn from other projects when they meet at conferences. He would learn how to navigate GDPR and ways of doing things that others have already tried. Viewing each project as individual systems, this would be a form of communication between systems, where communication is done through the conferences. However, the entire conference is taking place within the system of IoT development, meaning that it is a self-reproduction of the system by observing itself and its own operations. Where simply the subsystems are communicating with each other. This indicates that at least some of the communications, even with regard to things such as the GDPR is simply self-reproduction through self-observation.

When it does not, such as, regarding transparency, the system is more likely to look towards its own operations to understand how to navigate it. As a result, when two of the interviewees

were asked about their views on transparency, they answered how the project would make things they were measuring more transparent to them. A form of transparency that is typically outside of the concerns of the legal and academic systems. As the development of the technology was part of the systems operations but for these two projects the legal and academic systems regards to transparency were unobservable by them, the inspiration to the answers was instead completely self-referential. Referencing the systems own operations.

Other systems

The focus of this thesis is primarily on the communication between the system of IoT development with the legal and academic systems. However, it is clear from the interviews that communication with other systems is also influential to the operations of the system of IoT development, even pertaining to the ethical principles at hand. In the project directed towards healthcare, the interviewee said that the expertise of nurses they were working with was invaluable with regards to the issues of integrity and GDPR. Meaning that even with regards to the legal system the communication actually came from the healthcare system. He also mentioned experts from other areas giving their input into the project. It is also likely that a lot of the values of the interviewees comes directly from the greater social system or 'society'. Many of the answers that were given were pretty much in line with the general sentiment on these topics. Which is not strange or surprising, since everyone is part of that system, including everyone part of the system of IoT development. As such there is a clear structural coupling between the two systems. The same goes for the legal system which is strongly structurally coupled to the greater social system especially through the political system. Since the political system is democratic it has a vested interest in creating laws that are in line with the general sentiments. As such, it is likely that, at least parts of, the values the system of IoT development shares with the legal system, does not actually come from either but originates in another system and was adopted by both systems through the greater social system.

This means that there may be ways for the academic system and the legal system to communicate with the system of IoT development that are less direct. There may be systems which have a stronger structural coupling to both systems than they have to each other that could mediate the communication. The greater social system is one such system, since its values will often influence most other systems. It is however a system which, in the past, has proven difficult to directly influence. The system which is best at influencing it is probably the mass media system. It of course has structural couplings to both the legal and the academic

system. Through the mass media system, the academic system could attempt to influence the greater social system by highlighting the ethical issues with IoT in the form of interviews and in that way influence the system of IoT development. It is, however, a risky strategy as the mass media systems influence is strongest when it comes in the form of hyperbole, which runs the risk of damaging the reputation of the system of IoT development.

The academic system does also have a structural coupling with the legal system. Where it can lobby for laws and highlight problems that may need legislation. As we have seen, the system of IoT development pays more attention to the legal system than the academic system. As such, there is a chance that the academic system will have more success through that channel. But the question of how much influence the legal system actually has, still remains. The best solution may be to introduce a specialized mediating system in the form of ethical consultants. An ethical consultant to the IoT projects could be sure to be up to date on the latest research and could dive deep into the laws and regulations and would likely have the time and resources to do so. When a consultant is hired by the projects they could then read up on the project and know exactly what applies to the specific project. They would also accumulate experience by working for many different projects. The only question is whether there is room for an ethical consultant within the budget of smaller IoT projects.

Conclusions

There are clear ethical concerns with IoT. The diversity of applications of IoT makes it difficult to determine exactly where the ethical concerns lie. The sensors used in IoT range from simple thermometers to advanced cameras and detection devices. As a result, the concerns in one case, may not be a concern in another. Because many IoT applications are made to fit into a larger context and often aggregate data with other applications, it often unclear if initially harmless data should be of concern when aggregated with other data. Therefore, research on the topic is highly valuable to increase our understanding of how this technology will affect people's lives. There is, however, little point in doing research if the results of the research cannot reach the relevant parties so they can apply the research to the development.

From the interviews conducted for the purpose of this thesis, it became apparent that there are hurdles to the communication of these ethical principles. Rather than relying on the research, developers tend to look inwards and to each other when determining where the ethical lines should be drawn. They will reference draw references from each other or often from the common sense of the greater society. While people have a pretty good sense as to where the

lines should be drawn, there are some areas where the risks are not quite obvious enough for common sense to detect them. Regulations such as GDPR and Sweden's Camera Surveillance Act does serve as a guideline for the developers but are flawed in how the regulations are communicated. The laws are often in legalese and are difficult for people without education in law to fully understand. Interviewees even mentioned that lawyers had issues understanding them and when they were applicable. Since the laws are not written specifically with IoT in mind, it is often difficult to say exactly when the lines should be drawn and who is responsible when the project is only one part in what may eventually be in violation. Even with these issues, it seems as though the people working with IoT development are generally in line with the law in their views with regards to privacy and security, even when they are not using the law as reference. Transparency does have some issues however, the GDPR puts strong requirements on transparency. What exactly it means within the context of IoT is anything but clear. Even within the academic texts, most of the focus is on transparency of the data itself. But as one interviewee said: a lot of IoT detection is meant to be invisible. How are you supposed to be transparent when counting how many cars pass a bridge? Where exactly is the transparency required in such a case? It seems that the diversity of applications makes the transparency question very difficult.

It appears the academic system struggles to communicate its ideas to the system of IoT development. It is hard to say exactly why this is. It may be that the ways in which the academic system communicates, is inaccessible to large portions of the system of IoT development. Academic papers are not being read, and education is very slow. It may be that the academic system needs to find new ways of communication if they want to get its messages through.

There seems to be room for indirect communication using other systems. If the structural coupling is strong to both the system of IoT development and either the academic or the legal system, such a system may be used as a mediator for the communication. One needs to be careful, however. Depending on what the structural coupling looks like, there may be unintended consequences to using pre-established connections just to get a message through.

At the end the autopoiesis of the system makes absolutely necessary to consider the binary code of the system of IoT development if one wants to maximize the efficiency of communication. If it does not trigger the binary of beneficial/detrimental in the system, the system will either struggle to translate the communication properly, or in the worst case it may not be able to integrate the communication at all.

Suggestions

As has been made clear throughout this thesis, the communication of ethics between the legal system, academia and the development of IoT is not ideal and there is a lot of room for improvement. As it is right now each system has its own issues that are preventing proper communication. The issues with the legal system, is that the laws and regulations are rather broad and open for interpretation to because regulations such as the GDPR are meant to cover just about any form of data collection. As such, it becomes difficult for IoT developers to fully understand how they are meant to interpret the regulations and thus either require legal assistance or risk unintentionally violating the regulations. The variation of enforcement between EU member states further muddies the water. A solution to this issue would be to create guidelines or 'best praxis cases' specifically directed towards IoT where developers easily can understand how the regulations apply to their individual projects. Since this was a suggestion by the interviewees, there seems to be a need for it. One may not be enough however, given the wide diversity of IoT applications. In order to give clear guidelines and examples there may be a need for several covering different types of IoT to make sure that the developer knows exactly how the laws are applicable to their specific project.

The issue within the academic system is that there is so much being produced that it is hard to navigate and will take a lot of time to do so. A lot of the literature is also locked behind paywalls making it hard to access by IoT developers. Another issue is a separation within the academic system between different academic disciplines where IoT is mainly within the technological domain and ethics are more in the domain of social science or philosophy. Haven taken courses and talked to students from various technology programs I discovered that they study very little ethics as part of their curriculum outside of learning about GDPR. As such, some ways in which the academic system can improve is to increase the cooperation between scientific fields as technology is moving more and more into the social domain. Producing books or other forms of literature that consolidates the science surrounding ethics directed towards developers may also be useful. However, the best tool for communication in the academies' toolbox is education. Increasing the ethics education in tech development would transfer the knowledge through the students when they later start working with development.

The issue on the IoT development side is partially 'tunnel vision', where a focus on the development may cause the ethics to fall to the wayside. This is especially true with regards to transparency. As we saw in the interviews, questions about transparency sometimes gave

answers in line with the projects aims rather than in line with law or ethics. Another problem is that there often is not enough time for them to truly dive deep into the literature on ethics. The solution here could be to take at least a little bit of extra time to read up or think about the ethical implications, especially with regards to how the data may be used when consolidated with other data.

The best suggestion that would cover most of the current issues, is an implementation of ethics consultants directed towards IoT. There was a clear interest in the topic from the interviewees and seemingly a thirst for knowledge on the topic. As such, there should be an opening in the market for ethics consultants to fill. The advantage they would bring is an ability to be well read on both the law and the science. They would also be able to crosspollinate projects of various sizes with experience. The only question is whether there is room for ethics consultants with the budgets of the various projects. It should not be an issue with larger projects. Smaller ones are a bigger question.

Further research

The scope of this thesis was very limited. As a result, it is hard to draw any generalized conclusions. It should be viewed as an exploratory study to see any indications of the issues. In the future there is need for a much broader study with a larger sample size, to see whether the issues found in this thesis are widespread. It would also be interesting to see how these findings differ between countries, especially between different EU member states. Since this thesis was focusing on project managers, a study into other members of projects would be insightful. Especially given the limited insight the managers had into the security they implemented. A similar study with the people in charge of the security of IoT projects would be a natural complement to this thesis.

Furthermore, research could also expand into other ethical issues. GDPR includes regulations regarding accessibility and discrimination. Staying within the context of Luhmann, there is also room for research into the communication between the system of IoT development and other societal systems such as healthcare, education, political or the system of greater society.

There is also a lot of research currently being done on AI. As AI will likely be integrated into a lot of IoT projects there is also room for broader research into the relationship between AI and IoT and the possible ethical concerns that may arise from such an integration. Especially

when applied on a larger scale. A deep dive into a large IoT project such as smart city developments where one can fully analyze the entire project and interview several members of the team would be a good next step.

References

Alfandi, O., Khanji, S., Ahmad, L., & Khattak, A. (2021). A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. *Cluster Computing*, *24*(1), 37-55.

Alfandi, O., Khanji, S., Ahmad, L., & Khattak, A. (2021). A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. *Cluster Computing*, *24*(1), 37-55.

Beach, D., & Pedersen, R. B. (2019). *Process-Tracing Methods: Foundations and Guidelines* (2 ed.). University of Michigan Press.

Besio, C., & Pronzini, A. (2008). Niklas Luhmann as an empirical sociologist: Methodological implications of the sysyem theory of society. *Cybernetics & Human Knowing*, *15*(2), 9-31.

Brauneis, R., & Goodman, E. P. (2018). Algorithmic transparency for the smart city. *The Yale Journal of Law & Technology*, 103-176.

Bryman, A. (2016). *Samhällsvetenskapliga metoder (Social Research Methods Third Edition)* (3 ed.). (B. Nilsson, Trans.) Malmö: Liber AB.

Chanal, P., & Kakkasageri, M. (2020). Security and Privacy in IoT: A Survey. *Wireless Personal Communications*, *115*(2), 1667-1693.

Hydén, H. (2020). Chapter 28: Soiology of digital law and artificial intelligence. In J. Přibáň, *Research Handbook on the sociology of Law* (pp. 357-369). Cheltenham: Edward Elgar Publishing Limited.

ITU-T. (2012, 06). Overview of the Internet of Things: Recommendation ITU-T Y.2060. Internet Telecommunication Union.

Jiang, J., Kantarci, B., Oktug, S., & Soyata, T. (2020). Federated Learning in Smart City Sensing: Challenges and Opportunities. *Sensors*, *20*(6230), 6230-6230.

Lessig, L. (2006). *Code 2.0*. New York: Basic Books.

Liang, W., & Ji, N. (2022). Privacy challenges of IoT-based blockchain: a systematic review. *Cluster Computing*, *25*(3), 2203-2221.

Long, Y., Luo, X., Zhu, Y., Lee, K. P., & Wang, S. J. (2023). Data Transparency Design in Internet of Things: A Systematic Review. *International Journal of Human-Computer Interaction*, 1-23.

Luhmann, N. (1990). Technology, environment and social risk: a systems perspective. *Industrial Crisis Quarterly, 4*(3), 223-231.

Luhmann, N. (1991). Operational Closure and Structural Coupling: The Differentiation of the Legal System. *Cardozo Law Review, 13*(5), 1419-1442.

Luhmann, N. (1996). On the scientific context of the concept of communication. *Social Science Information, 35*(2), 257-267.

Luhmann, N. (1996). The Sociology of the Moral and Ethics. *Internal Sociology, 11*(1), 27-36.

Luhmann, N. (2012a). *Theory of Society Volume 1.* (R. Barrett, Trans.) Stanford: Standord University Press.

Luhmann, N. (2012b). *Theory of Society, Volume 2.* (R. Barrett, Trans.) Stanford: Stanford University Press.

Luhmann, N. (2013). *Introduction to Systems Theory.* (P. Gilgen, Trans.) Malden: Polity Press.

Matheus, R., Janssen, M., & Maheshwari, D. (2020). Data science empowering the public: Data-driven dashboards for transparent and accountable decision-making in smart cities. *Government Information Quarterly*, 1-9.

Mohamad Noor, M., & Hassan, W. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks, 148*, 283-294.

Nord, J. H., Koohang, A., & Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. *Elsevier*, 97-108.

Pires, Á., & Sosoe, L. (2021, 01 15). Epistemological and empirical challenges of Niklas Luhmann's systems theory: an interview with professors Álvaro Pires and Lukas Sasoe. (L. F. Amato, M. A. de Barros, & G. F. da Fonseca, Interviewers)

Rose, K., Eldridge, S., & Chapin, L. (2015). *The internet of Things: An Overview.* Geneva: Internet Society.

Syed, A. S., Sierra-Sosa, D., Kumar, A., & Elmaghraby, A. (2021). IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. *Smart Cities*, 429-475.

Vinnova. (2023). Vinnovas allmänna villkor för bidrag - 2023: En Projektpart (Vinnova's general terms for grants - 2023: One Projectpartner.

Wazid, M., Das, A., Shetty, S., & Jo, M. (2020). A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things. *IEEE Access, Access, IEEE, 8*, 88700-88716.

Appendix 1

Interview Guide

Interview Questions:

Berätta lite om dig själv och din bakgrund.
(Tell me a bit about your background)

Berätta lite om projektet.
(Tell me a bit about the Project)

Hur tänker ni implementera IoT?
(How do you intend to implement IoT?)

Är projektet byggt för att kunna integreras i en bredare struktur?
(Is the project meant to be integrated into a broader structure?)

Hur har ni diskuterat kring frågor som integritet, transparens och säkerhet?
(How have you discussed topics such as integrity (Privacy), transparency and security?)

Hur tänker du kring integritet i allmänhet?
(What are your thoughts about integrity (privacy) in general?)

Hur tänker du kring transparens i allmänhet?
(What are your thoughts about transparency in general?)

Hur tänker du kring säkerhet i allmänhet?
(What are your thoughts about security in general?)

Har ni funderat på dessa frågor i kontexten att det kan kopplas ihop med bredare system?
(Have you (the people in the project) given any thoughts to these topics within the context of a connection to a broader system?)

Hur har ni tagit hänsyn till lagstiftning och riktlinjer såsom GDPR?
(Have you given any considerations to legislations and guidelines such as GDPR?)

Tycker du att det skulle behövas mer lagar och riktlinjer?
(Do you think more laws and guidelines are needed?)

Ser ni något till vetenskaplig litteratur kring frågor om integritet, transparens och säkerhet?
(Are you considering any scientific literature surrounding topics such as integrity (privacy), transparency and security?)

Fick du läsa något om dessa principer i din utbildning?
(Did you read about these principles as part of your education?)

Appendix 2

Consent form

Samtycke i samband med intervju

Jag studerar på mastersprogrammet i rättssociologi på Lunds universitet och som del av mitt examensarbete undersöker jag hur projektledare för svenska projekt inom Internet of Things (IoT) tänker kring etiska principer såsom integritet, transparens och säkerhet. Jag vill därför intervjua dig i din yrkesroll som del av detta projekt. Med ditt godkännande skulle jag även vilja spela in intervjun så att jag sedan kan transkribera (skriva ut) hela samtalet. Inspelningen kommer att raderas så fort projektet är godkänt och betyget har registrerats.

Ditt deltagande kommer, till den grad det går, att anonymiseras i projektet, d v s ditt namn, din arbetsplats och andra uppgifter som kan identifiera dig kommer ej att framgå i projektet. Det är enbart jag, min handledare på universitetet och eventuellt en examinator/kursansvarig som kommer veta vem som blivit intervjuad. På grund av att urvalsgruppen projektledare för svenska projekt inom IoT är relativt liten, är det dock svårt att helt omöjliggöra identifiering.

Du kan när som helst återkalla ditt samtycke utan att ange orsak genom att kontakta mig via kontaktuppgifterna nedan. Ett återkallande påverkar dock inte den behandling som skett innan återkallandet. Jag kommer att spara ditt underskrivna samtycke så länge det är aktuellt, d v s fram tills inspelningen är raderad.

Vid frågor kan du alltid kontakta mig via följande uppgifter.

Namn på ansvarig student: Joakim Marklund

Kontaktuppgifter:
E-mail: [redacted]
Tel: [redacted]

Jag samtycker till inspelning av intervju och att den behandlas i enlighet med informationen ovan.

_____
Ort och datum

_____
Namnteckning

_____
Namnförtydligande

LUNDS UNIVERSITET