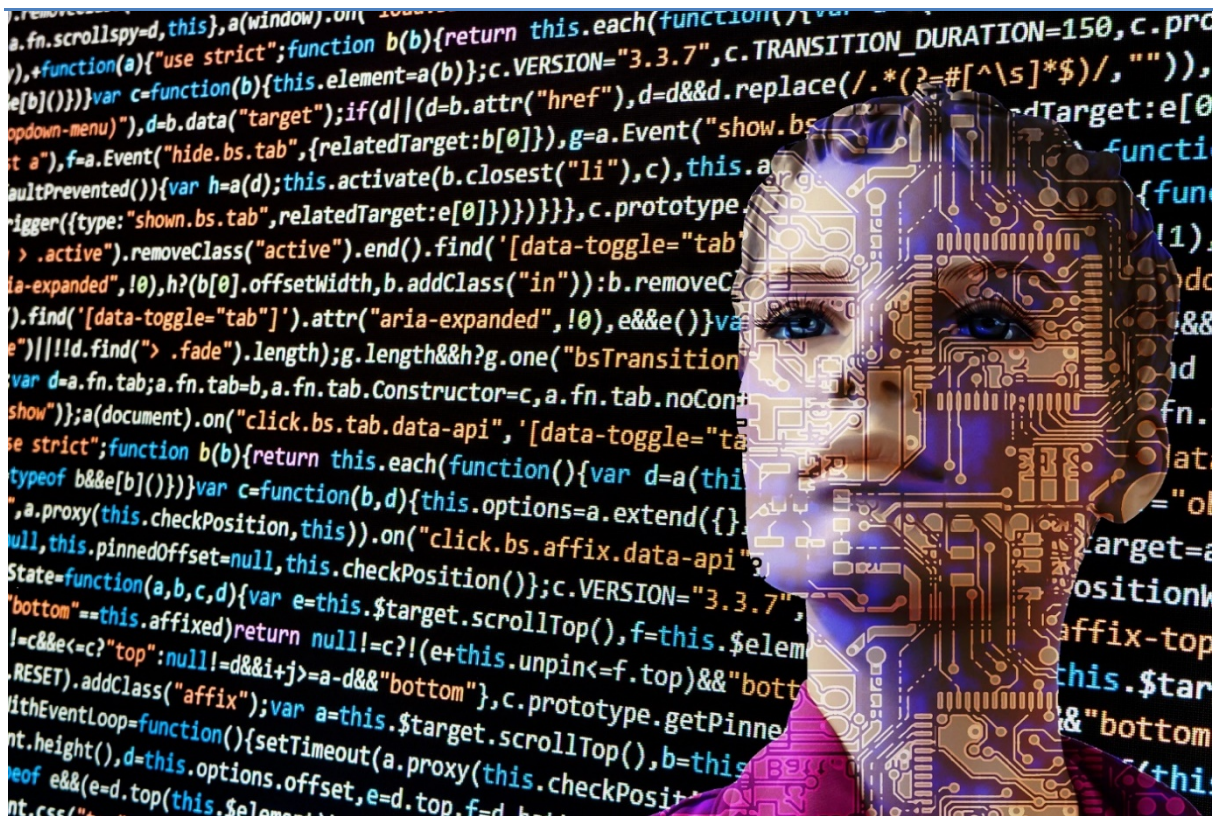




Case Study Introduction and Overview



This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641



Document Control

Deliverable	D1.1 Case Studies
WP/Task Related	WP 1: Representation and Visualisation
Delivery Date	31 January 2019
Dissemination Level	Public
Lead Partner	University of Twente
Contributors	Kevin Macnish, UT; Mark Ryan, UT
Reviewers	Bernd Stahl, DMU
Abstract	This report provides an overview of the methods employed to develop and manage the creation of 10 case studies
Key Words	Case studies, ethics, smart information systems, big data

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes
1	3/1/2019	K Macnish		First draft
2	22/1/2019	M Ryan		Second draft
3	28/1/2019	K Macnish		Case studies added

Contents

Executive Summary.....	4
Developing 10 Case Studies in Smart Intelligence Systems: An Overview	5
1. Background: Developing Criteria	5
2. Launch and Assigning Case Studies.....	7
3. Conducting Case Studies	18
4. Reporting on Case Studies	19
5. Conclusion.....	21
6. References	24
7. Appendices.....	24
8. The Case Studies	30
CS01 – Employee Monitoring and Administration	30
CS02 – Government	57
CS03 – Agriculture.....	84
CS04 – Sustainable Development	111
CS05 – Science	143
CS06 – Insurance.....	167
CS07 – Energy and Utilities	196
CS08 – Communications, Media and Entertainment.....	223
CS09 – Retail and Wholesale Trade	246
CS10 – Manufacturing and Natural Resources	269

Executive Summary

The SHERPA consortium looked at ten case studies that would give a broad overview of the many ethical issues faced in current use and implementation of smart information systems (artificial intelligence and Big Data). Smart information systems (SIS) offer businesses, governments, customers, and society as a whole, great potential and opportunity to increase profits, automate tedious jobs, improve services, and create advancements in knowledge and innovation. However, there are also many potential issues and concerns raised with emerging technologies. SIS are having a profound ability to shape and change the way we interact with the world and it is important to identify ethical issues being faced in different social domains.

While there are many cross-cutting and overarching themes and problems that need to be addressed in relation to the use of SIS, there are also many concerns that are domain-specific. The purpose of this SHERPA case study deliverable is to analyse a wide range of domains to identify the issues that are being faced in a number of ICT startups, research institutes, NGOs, public sector departments, and large ICT multinationals across Europe. This document will provide an overview of the process we undertook in identifying, collaborating, and constructing our case studies for this deliverable. It will consist of an overview of work package 1 and the ten case studies developed for its first deliverable, how these were chosen, and the steps taken to ensure high-quality results.

The case studies carried out were a part of the first work package in the SHERPA project form a backbone for the rest of the project. Along with the scenarios (WP1.2) they ground the analytic and stakeholder interaction in reality, reflecting the real-world situation regarding the employment of Smart Information Systems (SIS). While press and academic reports can tend towards sensationalism and scare mongering, with these case studies SHERPA brings the first large-scale empirically-grounded analysis of what is actually happening across a number of sectors in Europe, including government, health care, cybersecurity, telecommunications and insurance.

Each case study was designed in accordance with a mutually-developed protocol, which will be published as part of the work package. The protocol, coupled with ongoing regular conference calls, ensured a consistency of standards across the case studies. This in turn allows the case studies to be used for comparative analysis to assess the difference in uses of SIS by, for instance, different smart cities and telecommunications companies. Each case study then went through at least three rounds of peer review before being submitted to the Workbook and submission to the ORBIT journal.

Developing 10 Case Studies in Smart Intelligence Systems: An Overview

This overview report presents a summary of the actions taken for the SHERPA project (WP1.1). The case studies carried out are part of the first work package in the SHERPA project and form a backbone for the rest of the project. Along with the scenarios (WP1.2), they ground the analytic and stakeholder interaction in reality, reflecting the real-world situation regarding the employment of Smart Information Systems (SIS). These SIS case studies bring the first large-scale empirically-grounded analysis of what is happening across a number of sectors in Europe, such as government, health care, cybersecurity, telecommunications and insurance.

Each case study was designed in accordance to our case study protocol (section 2.4), which coupled with ongoing regular conference calls, ensured a consistency of standards across the case studies. This in turn allows the case studies to be used for comparative analysis to contrast SIS across an array of domains.

This overview report describes the development of the case studies, the timeline, and challenges and solutions encountered along the way. The report opens with the background work conducted on the case studies prior to the official launch of the SHERPA project in May 2018 (Section 1). It then looks at the development of the case study protocol, which formed the guidance procedure for the 10 case studies (Section 2). The report then considers how the case studies were conducted, in terms of both background and specific research, the interview process (Section 3), before turning to the qualitative analysis, report writing, and editing process (Section 4). The report concludes with considerations regarding challenges faced, lessons learnt and insights from the case study process (Section 5).

1. Background: Developing Criteria

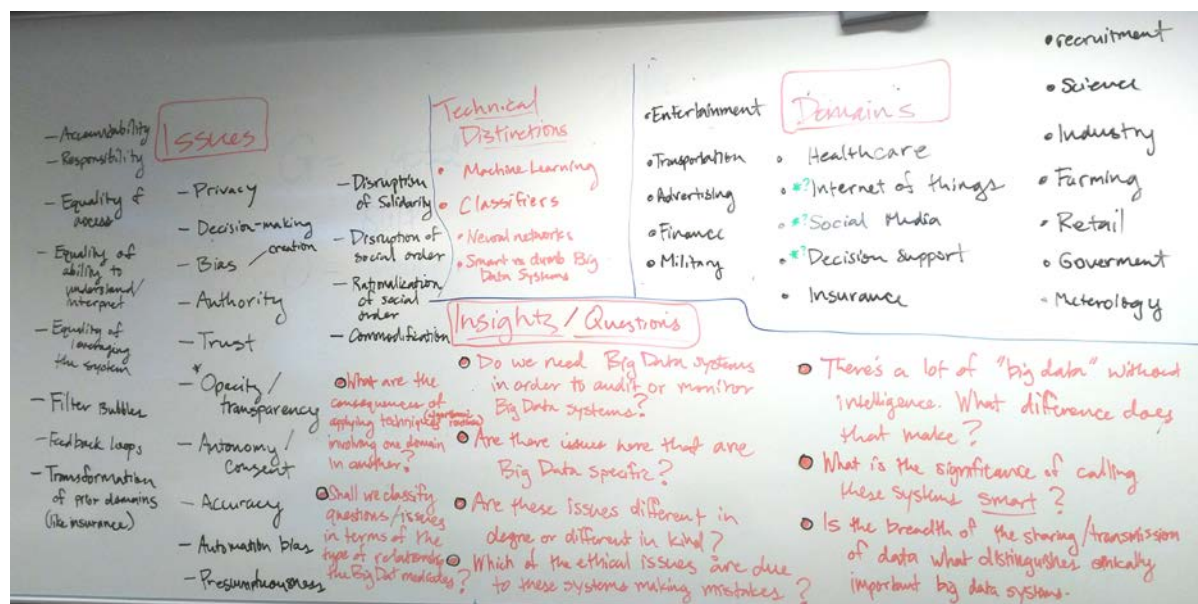
The process of case study development began in March 2018. Having successfully won the SHERPA contract, attention turned to understanding what would be involved in the case study process. It was decided that a number of criteria needed to be established early on to ensure the successful development and production of ten high-quality case studies. As the work package leader, the University of Twente (UT), created a process to distinguish the different types of case studies that should be carried out, a broad literature study of the main ethical issues in Big Data and artificial intelligence (AI) to determine possible concerns to be uncovered and addressed in the case studies, and the creation of an example case study for consortium partners to follow.

Several brainstorming sessions occurred at UT between March and April 2018 regarding the means of distinguishing the different case studies to effectively cover a broad reach of areas and ethical issues surrounding the use of SIS in practice (see Fig 1). One approach considered was to distinguish case studies by means of technical classification, and particularly by reference architecture.¹ Hence case studies could have been distinguished along the lines of relational versus non-relational, batch processing versus real-time processing, or data type, to list a few examples. A 2nd means of distinguishing case studies considered was by 'user type'. Hence case studies could have been distinguished by whether the user was an individual, a business, an individual within a business, or a process application. The 3rd means of distinguishing the case studies was by

¹ See <https://www.ibm.com/developerworks/library/bd-archpatterns1/>
<https://www.saama.com/blog/design-big-data-architecture-6-easy-steps/>
<http://www2.egr.uh.edu/~zhan2/ECE6111/class/BigDataSurvey2014.pdf>

application domain.² This focused on the field in which the SIS would be applied. Hence distinguishing features might include whether the application was a social network, a business system, or a part of the Internet-of-Things (IoT).

Fig. 1. Image of Brainstorming at University of Twente



Following further discussion, it was agreed that at the very least, case studies should include employees, consumers, citizens, and governments.³ The final set of case studies was then determined to encompass both targets and application domains, at least one case per type of data user, and a distribution of cases over the different technical categories. However, it was acknowledged that this would lead to an ideal situation, and one which may need to be tempered with the availability of willing case study participants. It was decided to establish a list of different social domains using and integrating SIS, with the attempt of covering a wide number of these areas within the case studies. The final agreed list of application domains can be seen in Table 1.

Having agreed the ideal list of application domains, attention turned to gaining a broad understanding of ethical issues currently faced across these domains. A literature review was carried out which approached both concerns with Big Data and AI in general and at the application level, which will also form an integral part of SHERPA's WP1.4. It was sent to partners to understand the many ethical issues surrounding SIS. Finally, a review of the technologies employed in Big Data and AI was also carried out, so that partners were provided with technical knowledge and understanding of SIS before conducting domain specific research for their case studies and also preparation for their interviews with experts in those areas (see WP1.4).

Alongside the literature review, UT carried out a review of the applications of SIS, along with a review of potential consortium partners who may be suitable for working on certain social domains from their expertise, research areas, and interests (prior to the May 1st launch date). Furthermore, UT also conducted a broad domain analysis of SIS applications. Through a combination of desktop research and personal contact lists, UT identified a number of organisations from the 16

²<http://www1.unece.org/stat/platform/display/bigdata/Classification+of+Types+of+Big+Data>

³<https://www.ap-institute.com/big-data-articles/how-is-big-data-used-in-practice-10-use-cases-everyone-should-read>

social domains that use and integrate SIS in Europe. This list was distributed to SHERPA consortium partners as a suggestion of organisations to use for their case studies. Finally, an example case study was developed on Google DeepMind and the Royal Free Trust and was shared before the project launch in Brussels in May 2018.

Table 1: Social Domains Identified

Social Domains
Banking and securities
Healthcare
Insurance
Retail and wholesale trade
Science
Education
Energy and utilities
Manufacturing and natural resources
Agriculture
Communications, media and entertainment
Transportation
Employee monitoring and administration
Government
Law enforcement and justice
Sustainable development
Defence and national security

2. Launch and Assigning Case Studies

The project launch took place on May 1st, 2018 in Brussels, Belgium. At the launch, significant time was given to the introduction and discussion of the case studies within WP1. The main objective to be achieved at the launch was to discuss what the case studies should look like and to understand the potential domain interests of the consortium partners. We also discussed if partners had contacts in those domains or could think of organisations that would be suitable case study participants. This section will describe the outcomes from the launch event itself, the process of agreeing the case studies, and the development of the Case Study Protocol.

2.1. Launch

At the launch event in Brussels the example case study was presented, alongside the application domains. There was considerable discussion as to which domains partners should focus on, alongside concerns from some partners about their roles in the work package. A number of partners demonstrated apprehension about their involvement, despite being allocated time to work on the case studies, owing to their particular strengths and weaknesses. The launch presented an opportunity to connect with different partners and understand respective interests.

One challenge with the launch event was that not every person working on the project was in attendance. Several people who ended up working on the case studies were not physically present at the Brussels event. Despite this, the case studies developed quite significantly after the initial discussion at the launch event. UT were aware that the case studies would take on an evolutionary transformation during the process, but wanted to use this event to establish working relationships among the consortium and to establish areas of interests among the partners.

2.2. Agreeing Case Studies

One of the objectives at the launch event was to correlate partner interests and connections with the application domain criteria which had been developed by UT in advance. This formed a part of the WP 1.1 presentation in Brussels, which gave partners 20 minutes to identify application domains they were interested in, whether they would work alone or with another consortium partner, and what establishing possible organisations they could conduct their case studies on.

Once the application domains had been agreed by the consortium, a further decision was taken about whether certain application domains should be used as case studies (see Table 2) or scenarios (see Table 3). This was determined by partners' interests, competencies, and contacts, but also by a realistic assessment about which domains would fit better as a case study or scenario. For example, defence and national security was determined to be better suited as a scenario, because of the potential difficulty with finding suitable participants. By contrast, cyber security, in which one of the consortium partners was a dedicated expert, was deemed to be more suitable as a case study.

Also agreed at the launch event was the amount of person months (PM) available to work on the case studies. This averaged out at a maximum of 1.85 PM per case study, given that the Grant Agreement required a minimum of 10 case studies to be completed. As a result of uneven PM distribution, many of the consortium partners identified shared interests, co-authoring some of the case studies. Finally, it was agreed that case study authors should participate in weekly Skype conversations (Thursday mornings at 10.00 CET), chaired by the University of Twente.⁴

Some of the case studies try to provide a broad analysis of a particular domain, most of the case studies delved into a specific area or topic within their domain of choice in order to provide a more detailed and interesting case study. For example, some case studies focused on one organisation to provide a broad overview of some SIS issues in that domain, such as: BASF for agriculture (CS03) and Liander for energy (CS07).

⁴ These were managed by the WP 1.1 leader, who sent out an agenda and took minutes for each meeting. These weekly meetings ran from late May 2018 until late November 2018, with a final meeting held in early January 2019 to respond to the QA process. At a minimum, each meeting consisted of a review of the minutes from the prior meeting, follow-up actions, and a checking in process with each of the case study authors present on the call. This led to a degree of accountability among the case study authors, as well as an opportunity to share surprising or interesting findings that had been unearthed during the research or interview process.

While other case studies focused on a particular category within that domain to provide a more nuanced examination of SIS in that area, such as: a municipality for the government case study (CS02); smart cities as an aim within the Sustainable Development Goals (CS04); a large scientific research project (CS05); health insurance (CS06); and a supply-chain management risk prevention company (CS10).

Some of the case studies focused on specific applications, technologies, or departments within their domain of research: Internet-of-Things for employee monitoring (CS01); customer relations management in retail (CS09); and the use of SIS in cybersecurity department of a telecommunications provider (CS08). Overall, the case studies cover a wide range of areas, domains, specialisations, technologies, and approaches in the use and implementation of SIS, but were still able to provide cohesion and scientific rigour by following the case study protocol we completed before the case studies commenced.

Table 2: Case Study Division

No.	Case Study Social Domain	Partner(s)
CS01	Employee monitoring and administration	UCLanCY ⁵ and AHR ⁶
CS02	Government	UT
CS03	Agriculture	UT
CS04	Sustainable development	UT and EBS ⁷
CS05	Science	DMU ⁸
CS06	Insurance	EUREC ⁹
CS07	Energy and utilities	Trilateral
CS08	Communications, media and entertainment	UT and F-Secure
CS09	Retail and wholesale trade	UT and F-Secure
CS10	Manufacturing and natural resources	DMU

Table 3: Scenario Division

No.	Scenario Social Domain	Partner(s)
SC01	Healthcare	Trilateral
SC02	Defence & National Security	Trilateral
SC03	Education	UCLanCY and Trilateral
SC04	Transportation	UT

⁵ University of Central Lancashire Cyprus.

⁶ Aequis Human Rights.

⁷ European Business Summit.

⁸ De Montford University.

⁹ European Network of Research Ethics Committees.

SC05	Law Enforcement and Justice	UT and Trilateral
------	-----------------------------	-------------------

2.3. Developing Case Study Protocol

The case study protocol was created to guarantee consistency of approach and timeliness of the case studies. Development of the case study protocol fell primarily on UT (leaders of the case study deliverable), Trilateral (leader of the work package) and DMU (project coordinator). Both DMU and Trilateral also had significant experience in the development of case studies. UT carried out a preliminary literature review on the methodology of case studies for the case study protocol.

The protocol initially implemented a positivist approach to the research question – an initial hypothesis, which could later be confirmed or denied. In discussions held in mid-July 2018, it was pointed out that the interpretative approach suited the goal of the case studies better than the positivist approach, and thus this methodology was adopted.

A compromise needed to be agreed between an ideal number of interviewees, the ability to find willing participants, and the time constraints of the work package. In the end, a minimum number of one interviewee was agreed upon – if that individual was knowledgeable on both the technical and ethical use of SIS – with a recognition that two or more interviewees would be better.

The case study protocol was officially agreed on 16th August 2018, outlining a specific breakdown of tasks and deadlines to ensure successful completion of 10 case studies by January 31st (see Table 4).¹⁰ Following the finalisation of the protocol, a promising case study was identified to be used as a pilot (agriculture case study). This pilot served as the template to ensure consistency of style and format, as well as common approaches to content. In addition, case study authors were required to upload interview transcripts to NVivo¹¹ for analysis. This meant that DMU needed to buy additional licences for NVivo and make a secure DMU server available to authors.

A final consideration was the need for ethics approval by research ethics committees at participating universities (UT, DMU, University of Central Lancashire Cyprus). UT submitted the case study protocol to the University's research ethics committee in July 2018, and received a favourable response within 2 weeks. This allowed for the case studies to be carried out by UT with full ethical approval, as well as case studies by non-university partners. The other universities needed to gain ethics approval from their own research ethics committees. Given that research ethics approval is required prior to interviews taking place, it was important that the research ethics process was completed by the end of July 2018.¹² A significant aspect of gaining ethics approval was the

¹⁰ Deadlines for each component of the case study needed to grapple with the long summer break, the Christmas holidays, and a relatively short amount of time in January to finalise the case studies. Taken together, this meant that interviewees needed to be identified and contacted prior to mid-July in order to be sure of interviews conducted in September. The September deadline was important in order to have a first draft of the case study ready for the end of October, which could then be peer-reviewed at UT by the end of November. This would allow for approximately 3 weeks to respond to the peer-review process by each author, before passing the case study to the Quality Assurance Officer in January, still allowing time for final edits before the end of the month.

¹¹ NVivo is qualitative data analysis software from QSR International.

¹² In addition, in July, the authors of the case studies in WP1.1 were also approached by the leader of WP 2.2, who wished to use the information and interviewees from WP 1.1 as part of the stakeholder analysis process in WP 2. Some concern was raised among the authors that this might lead to volunteers for the interviews becoming overburdened with requests for information from the SHERPA project. However, it was decided that the transcripts of the interviews, published in a secure online server accessible to the leader of WP 2.2 would be sufficient for the purposes of the later work package.

development of a consent form and information sheet as part of the case study protocol, which could be used by partners prior to conducting interviews (see Appendix 7.1 and 7.2).

Table 4: Research Plan

Deadline	Task
27/06/2018	Identify partner's Principal Investigator/POC and Co-Investigator/Deputy POC for case study
13/07/2018	<ol style="list-style-type: none"> 1. Get ethics board approval for study (if available) 2. Identify interviewees (interviewee should have good technical knowledge about the structure and use of SIS in the organisation) 3. Approach contact(s) - explain purpose of study, nature of study, likely questions, arrange interview date/time
20/07/2018	Confirm agreement with organization(s) to participate in case studies in writing
03/08/2018	Carry out preliminary background research on organisation and its use of SIS
31/08/2018	<ol style="list-style-type: none"> 1. Complete Case Study Protocol Template for organisation 2. Carry out detailed background research on organisation's use of SIS
07/09/2018	Obtain written informed consent from interviewees
21/09/2018	Conduct interview(s)
28/09/2018	<ol style="list-style-type: none"> 1. Transcribe interviews 2. Upload transcriptions and other data to repository
12/10/2018	Conduct preliminary analysis (see guide for final report, below)
26/10/2018	<ol style="list-style-type: none"> 1. Write up draft report using template 2. Send draft report to interviewee(s) for validation (i.e. check our view that what they said is the same as their views on what they were saying). Allow for 2 weeks turnaround.
09/11/2018	Send agreed draft report to UT
30/11/2018	Discuss draft report with UT
21/12/2018	Write up final report using template and send to UT and the QA officer
14/01/2019	Discuss final revisions with QA officer
31/01/2019	UT to undertake cross-case analysis and compile final report

2.4 Case Study Protocol

We used exploratory case studies to uncover ethical issues which arise through the use of SIS across a number of different types of organisations. From the individual case studies, we will take a cross-case analysis to build a matrix of ethical issues experienced by different organisations. The primary research question was: How do organisations perceive ethical concerns related to SIS and in what ways do the organisations deal with them?

We believed that there would be discrepancies between how companies deal with the ethical considerations related to the SIS they employ. While some companies would search for the ethical considerations and deal with them well, some would search for them and deal with them poorly, others would search for them and not find any (even though they are present), while a fourth group would not search for them at all. We wanted to gain evidence from each of these cases to address the empirical plausibility of the research question.

2.4.1 Epistemology

Researchers need to decide on the research approach that most accurately addresses their research questions. Epistemology is a viewpoint about the nature of enquiry, the kind of knowledge discovered or produced, and the kind of strategies that are consistent with this (Becker and Niehaves, 2007). Our research sought to understand the ethical and human rights issues arising from SIS from the perspective of those developing it. Our case studies adopted an interpretivist approach, which allowed for both rigour and flexibility (Walsham 1995). It enabled researchers to empathise with research participants and seek to elicit insights, rather than an objective truth. This allowed us to understand 'reality' as the blending of the various (and sometimes conflicting) perspectives which coexist in social contexts, the common threads that connect the different perspectives and the value systems that give rise to the seeming contradictions and disagreements around the topics discussed. Whether one sees this reality as static (social constructivism) or dynamic (social constructionism) was also a point of consideration, as they both belong in the same "family" approach where methodological flexibility is as important a value as rigour.

With interpretivist approaches, it is often difficult for novice researchers to maintain consistency and coherence, as is for untrained evaluators to assess its rigour. Explicating the methods, protocols and procedures to be followed, as well as the reaching a common understanding of the semantics that underlie the research is of paramount importance. Hence, the following section explains in detail the methodology employed for the collection and analysis of the research material and their synthesis with the view to theorise around the ethical and human rights issues arising from SIS.

2.4.2 Methodology

The methodology that was used to answer the research question would be through qualitative case studies (Yin, 2015, 2003). As such the case study is defined by the interest in individual cases, which are the object of the research (Stake, 2005). The cases that were used in the SHERPA project were contemporary and complex functioning units, investigated in their natural context. The essence of using a case study methodology is that it allows for triangulation in coming up with a matrix of ethical issues experienced by different cases. Also, the qualitative case study methodology was ideal because of the descriptive and exploratory nature of the research which is dominated by 'how' and 'what' questions in gaining insights on the ethical issues that result from SIS and how they are dealt within respective cases.

We looked for diverse examples of SIS use which will highlight both common issues and anomalous issues across the cases. Each case study is exploratory, aiming to uncover the insights of organisational representatives on the matter and possibly the position of their organisation as a

result. The case studies adopted an interpretivist approach, which allows for rigour in the methodology, but also for the required flexibility (Walsham 1995). The unit of analysis for each case study was the use of SIS in the organisations (cases) investigated, be these corporate, governmental, NGO, project or other. We examined the cases from multiple lenses and levels of analysis (Rowley, 2002) in order to provide a holistic understanding across organisational levels, disciplines and technology domains.

2.4.3 Data Collection

In order to explore how different cases or organisations perceive ethical concerns related to SIS and in what ways they deal with them, the following types of data sources were used:

- Documents (e.g. organisation website and publications, company records, project documents and memoranda, illustrative materials (newsletters, publications that form part of the history), archival records) (see Table 5)
- Interviews (at least 2, open-ended, semi-structured, questions below - face-to-face is best, otherwise telephone/Skype) to be transcribed (see Table 6)

There was a minimum of one interview per case study from different professional disciplines (i.e. a business representative and an IT representative). It was important to address the interview questions to those most able to answer them (e.g. a Chief Technical Officer - CTO). However, in most cases, it was also valuable to speak to a Policy Advisor or others at the organisation who can address the impact of the technology on society. In some cases, the CTO was in a position to address all of the questions sufficiently (e.g. the government case study). Beyond the interview(s), supporting/supplementary information was required to develop a contextual understanding of the case study and lend credence to (or criticise) the responses of the interviewee.

Table 5: Desk Research Questions

Number	Research Question
1	In which sector is the organisation located (e.g. industry, government, NGO, etc.)?
2	What is the name of the organisation?
3	What is the geographic scope of the organisation?
4	What is the name of the interviewee?
5	What is the interviewee's role within the organisation?

Table 6: Interview Research Questions

No	Research Question
1	What involvement has the interviewee had with SIS within the organisation?
2	What type of SIS is the organisation using? (e.g. IBM Watson, Google Deepmind)
3	What is the field of application of the SIS (e.g. administration, healthcare, retail)
4	Does the SIS work as intended or are there problems with its operation?

5	What are the innovative elements introduced by the SIS (e.g. what has the technology enabled within the organisation?)
6	What is the level of maturity of the SIS? (i.e. has the technology been used for long at the organisation? Is it a recent development or an established approach?)
7	How does the SIS interact with other technologies within the organisation?
8	<p>What are the parameters/inputs used to inform the SIS? (e.g. which sorts of data are input, how is the data understood within the algorithm?)</p> <ul style="list-style-type: none"> Does the SIS collect and/or use data which identifies or can be used to identify a living person (personal data)? Does the SIS collect personal data without the consent of the person to whom those data relate?
9	<p>What are the principles informing the algorithm used in the SIS (e.g. does the algorithm assume that people walk in similar ways, does it assume that loitering involves not moving outside a particular radius in a particular time frame?)</p> <ul style="list-style-type: none"> Does the SIS classify people into groups? If so, how are these groups determined? Does the SIS identify abnormal behaviour? If so, what is abnormal behaviour to the SIS?
10	Are there policies in place governing the use of the SIS?
11	How transparent is the technology to administrators within the organisation, to users within the organisation?
12	Who are the stakeholders in the organisation?
13	What has been the impact of the SIS on stakeholders?
14	How transparent is the technology to people outside the organisation?
15	<p>Are those stakeholders engaged with the SIS? (e.g. are those affected aware of the SIS, do they have any say in its operation?)</p> <p>If so, what is the nature of this engagement? (focus groups, feedback, etc.)</p>
16	In what way are stakeholders impacted by the SIS? (e.g. what is the societal impact: are there issues of inequality, fairness, safety, filter bubbles, etc.?)
17	What are the costs of using the SIS to stakeholders? (e.g. potential loss of privacy, loss of potential to sell information, potential loss of reputation)
18	What is the expected longevity of this impact? (e.g. is this expected to be temporary or long-term?)

19	What has been the impact of the SIS on stakeholders?
20	Are those stakeholders engaged with the SIS? (e.g. are those affected aware of the SIS, do they have any say in its operation?)
21	If so, what is the nature of this engagement? (focus groups, feedback, etc.)
22	In what way are stakeholders impacted by the SIS? (e.g. what is the societal impact: are there issues of inequality, fairness, safety, filter bubbles, etc.?)
23	What are the costs of using the SIS to stakeholders? (e.g. potential loss of privacy, loss of potential to sell information, potential loss of reputation)
24	What is the expected longevity of this impact? (e.g. is this expected to be temporary or long-term?)

2.4.4 Recording and management of data

The interviews were recorded using a suitable tool that allowed access in a broadly accessible format (e.g. mp3). All interviews were transcribed by the researcher or by a reputable third-party company (UKTranscription). The individual undertaking the interview had to confirm and validate the transcription. Once the interview data has been analysed, the researcher deleted the audio recordings. All data including the interview transcripts were stored and logged in secure group repository (WordPress and NVivo). The audio files were deleted, once the analysis of the interview was completed.

2.4.5 Data analysis

The collected data was analysed using a thematic analysis technique. In using a thematic analysis, we were able to highlight, expose, explore, and record patterns within the collected data. The themes are patterns across data sets that are important to describe several ethical issues which arise through the use of SIS across a number of different types of organisations. In addition, NVivo was used as a tool for the data analysis. UT will also engage in a cross-case analysis of the ten different case studies, which will draw together ethical issues arising in the ten case studies. This will then form the backbone for the ethical analysis in WP1.4.

2.4.6 Guide for Final Report

Each case study culminated in a final report consisting of an analysis and identification of core ethical issues that arise in the case study. The issues included likely and unlikely ethical concerns (see Table 7). For consistent reporting across the 10 case studies, a template for the final report was provided (see Appendix 7.3).

Table 7: Checklist of Ethical Issues

Ethical Issue	Question Example	✓
Privacy	Does the use of the technology raise concerns that people's privacy might be at risk or endangered?	
Personal Data	Does the technology or its use presume a particular group or person "own" the data? If so, who?	

Security	Does the technology use personally-identifying data? If so, is this data stored and treated securely?	
Inclusion of stakeholders	Are people affected by the technology involved in any way with its use or implementation? Do they have an opportunity to have a say in how the technology impacts them?	
Consent of stakeholders	Have people affected by the technology been given an opportunity to consent to that technology existing or having the impact that it does on their lives?	
Loss of employment	Does the use of the technology put people's jobs at risk, either directly or indirectly?	
Autonomy/agency	Does the use of the technology impact in any way on people's freedom to choose how to live their lives?	
Discrimination	Can/does the technology or its use lead to discriminating behaviour in any way? Does the technology draw on data sets that are representative of those stakeholders affected by the technology?	
Potential for military/criminal/ nefarious use	Could the technology be used for military, criminal or other ends which were not envisaged or intended by its developers?	
Trust	Does the technology impact people's trust in organisations, other people, or the technology itself?	
Power asymmetries	Can or does the technology exacerbate existing power asymmetries by, for instance, giving a large amount of power to those already holding power over other people?	
Inequality	Can or does the technology reduce inequalities in society or exacerbate them?	
Fairness	Is the technology fair in the way in which it treats those affected by it? Are there unfair practices which arise in relation to the technology?	
Justice	Does the technology or its use raise a feeling of injustice on the part of one or more groups affected?	
Freedom	Does the technology or its use raise questions regarding freedom of speech, censorship, or freedom of assembly?	
Sustainability	Is the technology or its use sustainable, or does it draw on limited natural resources in some way?	

Environmental impact	Does the technology have any impact on the environment, and if so what?	
----------------------	---	--

2.4.7 Outline of narrative

The final report took a narrative structure. In constructing the final report, partners addressed the hypothesis to avoid drowning in the data (there were many aspects arising in the course of the research which were not strictly pertinent to the ethical issues in the case study). The analysis rested on all of the relevant evidence, rather than “cherry picking” certain aspects. For instance, it may be possible to see a privacy violation occurring, but the organisation in question may have also recognised this and taken steps to resolve it. In such cases, both the potential violation and the mitigation were noted. This was not intended to be a comprehensive report on everything uncovered in the course of the research, but a report on the ethical issues. Ultimately, “the goal of the report is to describe the study in such a comprehensive manner as to enable the reader to feel as if they had been an active participant in the research and can determine whether or not the study findings could be applied to their own situation. It is important that the researcher describes the context within which the phenomenon is occurring as well as the phenomenon itself.” (Baxter & Jack 2008, p555).

2.4.8 Potential Issues

We identified a number of potential issues that were to be addressed during the interviews, qualitative analysis and writing up of the reports (see Table 8).

Table 8: Potential Issues

Issue	Explanation of Issue
Unbounded	We are interested in ethical issues arising from the use of SIS in organisations. Hence, we want information relating to the use of SIS and ethical issues that the organisation has recognised and either dealt with or chosen to ignore
Incomparable	It is extremely important that the case studies be comparable. We are therefore adopting a positivist framework and using this case study protocol to inform the design of every case study to ensure comparability. This will be supplemented by bi-weekly meetings to discuss progress and share experiences. "The rigour of case studies should therefore be judged by the same criteria [as any other empirical, scientific method] of internal validity, external validity, construct validity, and reliability" (Yin 1992 p124)
Contact does not have access to relevant material	Raw data is highly valuable in these case studies to allow for developed analysis. However, it is accepted that this may not be available (or shareable with us). In those cases, focus will be placed on issues faced and dealt with (or not as applicable) by the organisation.
Understanding issues	All case studies will be preceded by the principal investigator conducting background reading of Yin (1992), Mittelstadt et al (2014) and Macnish (2010) to gain an understanding of the purpose of the case study (Yin 1992), the range of

	issues currently identified in use of algorithms (Mittelstadt et al 2014) and an example of how analysis of an algorithm's parameters can lead to ethical concerns (Macnish 2010).
--	--

3. Conducting Case Studies

Conducting the case studies involved carrying out background research, both generic regarding the application domain, identifying interviewees, and research on the organisation(s) that they belong to, and conducting the interviews. These stages lasted from June 2018 (the beginning of general background research) until October 2018. UT rigorously kept track of partners' progress, through an Excel Matrix, throughout this process to ensure deadlines were met (see Fig 2).

Fig 2: Case Study Progress

No	Case Study	Partner	POC	dPOC	13/7/2018 IRB Approval	13/7/2018 Interviewee(s) Approached	20/7/2018 Participation Confirmed in Writing	20/7/2018 Roles of Interviewee(s)	3/8/2018 Preliminary Background Research Completed	31/8/2018 Case Study Protocol Template Started	31/8/2018 Detailed Background Research Completed	7/9/2018 Written Informed Consent from Interviewee(s) Obtained	21/9/2018 Interview(s) Conducted	28/9/2018 Interview(s) Transcribed and uploaded
1	Employee Monitoring (IoT)	UCLanCY & AHR	Josephina	Andreas	X	X	X	X	X	X	X	X	X	X
2	Government (municipalities)	UT	Mark	Kevin	X	X	X	X	X	X	X	X	X	X
3	Agriculture (agribusiness)	UT	Mark	Kevin	X	X	X	X	X	X	X	X	X	X
4	Sustainable Development (smart cities)	UT/EBS	Mark	Anyia	X	X	X	X	X	X	X	X	X	X
5	Science (Human Brain Project)	DMU	Tilimbe	Bernad	X	X	X	X	X	X	X	X	X	X
6	Insurance (Health)	EUREC	Natalija	Lisa	-	X	X	X	X	X	X	X	X	X
7	Energy (Smart Grid)	TRI	Tally	Rowena	-	X	X	X	X	X	X	X	X	X
8	CRM (Telecoms)	UT/F-SEC	Kevin	Alexey	-	X	X	X	X	X	X	X	X	X
9	Telecoms (Cybersecurity)	UT/F-SEC	Kevin	Alexey	-	X	X	X	X	X	X	X	X	X
10	Manufacturing (SCM)	DMU	Tilimbe	Bernad	X	X	X	X	X	X	X	X	X	X

3.1. General Background Research

For each case study, existing as it did in its own application domain, general background research needed to be carried out. This came in addition to the more general research on ethical issues in Big Data carried out by UT prior to the start of the project. For each case study, the author investigated articles on ethics and legal issues for the particular application domain across a range of media. These included academic journals, trade journals, and Internet searches. In the process of the background research, both primary and secondary interview candidates were identified and contacted. Once initial contact had been established, permission for an interview was sought, alongside sending the potential interviewee the case study protocol, an information sheet, and a consent form (see Appendix 7.1 and 7.2).

3.2. Specific Background Research

Once interested persons had been identified and confirmed to be interviewed, more targeted background research could be conducted. This research focused on the particular company or organisation to which the interviewee belonged. The specific background research enabled the case study author to gain a fuller understanding of the issues faced by the organisation which was to form a part of the case study and to be informed of likely issues during the interview. It also meant that the interviewer could incorporate questions retrieved from their background research into the interview, rather than solely following the research questions from the case study protocol.

3.3. Conducting Interviews

Where possible, interviews were conducted at the place of work of the interviewee, so that they felt comfortable and were not inconvenienced by travel. Provision had been made for interviews to be held over Skype or by phone, in instances where an interviewee was too far away, or they opted to do it remotely. The interviewer(s) provided the information sheet and consent form to the

participant days or weeks before the interview, and also prior to the commencement of the interview itself. These were explained to the interviewee before they signed the consent form.

One issue which was not discussed in advance, and from which the case studies would have benefited, was an interview methodology. Several of the case study authors had little or no experience in conducting social science interviews. As a result, some case studies were based on an interview following the precise questions found in the case study protocol, while other case studies took a more open interview style, covering many topics but in a less dogmatic way than indicated in the protocol. Furthermore, some interviews were carried out on a strictly one-on-one basis, while others were conducted in a workshop format involving one or two interviewers and up to three interviewees (for example, the telecommunications case study).

Over time, a high degree of flexibility was also required: Organisation who had nominally agreed to be interviewed pulled out (social media case study); some application domains were very difficult to find willing interviewees (energy case study); while some domains even proved to be impossible to find participants (banking & finance). These challenges were countered by changing organisations to those who were willing to be interviewed or changing the domain area entirely.

3.4. Reflection

Following each interview, the case study author scanned and uploaded a copy of the signed consent form to a central secure location on our website. UT ensured that all documents were uploaded by the partners and that it was clear what the interviewees had consented to in their agreement. Notes from each interview were consolidated, and a thank you email sent to each interviewee. They were also informed that they would receive a first draft of the report once it was complete.

4. Reporting on Case Studies

The reporting process on the case studies began in October 2018. This consisted of having each interview transcribed and analysed in NVivo. Following this, a draft of the full case study was composed and sent to the interviewee for confirmation. The draft was then sent to WP 1.1 leader (UT) for peer-review. The review document was then returned to the initial author, who had until the end of December to return a final draft. This draft was then submitted for the QA process in January 2019, which resulted in further edits being required from each case study author by mid-January. Finally, the final version was sent to the deliverable coordinator in the last week of January. This enabled the writing of the final report by the deadline of 31 January 2019 (see Fig 3).

Fig 3: Progress chart

No	Case Study	Partner	POC	dPOC	12/10/2018 Preliminary Analysis Conducted (at NVivo workshop)	26/10/2018 Draft Report Written	26/10/2018 Draft Report Sent to Interviewee(s)	31/10/2018 Coding in Nvivo Complete	9/11/2018 Draft Report Sent to UT	30/11/2018 Draft Report Discussed with UT	21/12/2018 Final Report Sent to UT	31/1/2019 Final Report Written by UT
1	Employee Monitoring (IoT)	UCLanCY & AHR	Josephina	Andreas	X	X	X	X	X	X	X	X
2	Government (municipalities)	UT	Mark	Kevin	X	X	X	X	X	X	X	X
3	Agriculture (agribusiness)	UT	Mark	Kevin	X	X	X	X	X	X	X	X
4	Sustainable Development (smart cities)	UT/EBS	Mark	Anya	X	X	X	X	X	X	X	X
5	Science (Human Brain Project)	DMU	Tilimbe	Bernd	X	X	X	X	X	X	X	X
6	Insurance (Health)	EUREC	Natalija	Lisa	X	X	X	X	X	X	X	X
7	Energy (Smart Grid)	TRI	Tally	Rowena	X	X	X	X	X	X	X	X
8	CRM (Telecoms)	UT/F-SEC	Kevin	Alexey	X	X	X	X	X	X	X	X
9	Telecoms (Cybersecurity)	UT/F-SEC	Kevin	Alexey	X	X	X	X	X	X	X	X
10	Manufacturing (SCM)	DMU	Tilimbe	Bernd	X	X	X	X	X	X	X	X

4.1. Transcription

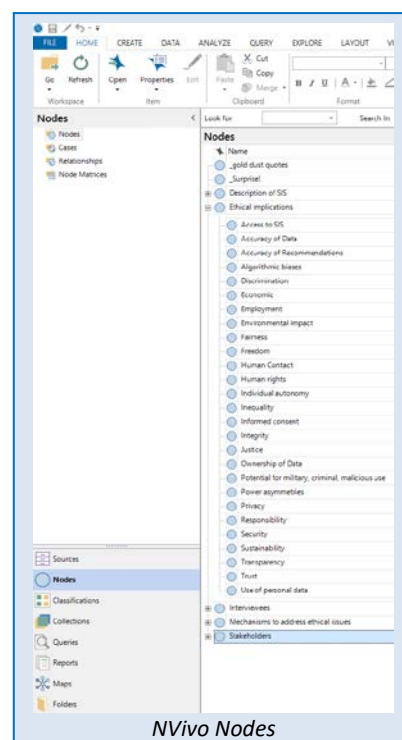
While each partner was nominally responsible for the transcription of their interview(s), a transcription service was identified which could transcribe the interviews quickly and at a very competitive price (UKTranscription). This company was recommended by several of the partners

within the consortium and had a strong track-record in the industry. The structure of these transcriptions also allowed partners to analyse their data in a more consistent way in NVivo.

4.2. NVivo

A workshop was arranged at DMU for the 2nd week of October to introduce case study authors to NVivo and provide a focused period of time for the transcribed interviews to be analysed. The workshop environment meant that the methodology for using NVivo (such as whether to encode concepts or precise phraseology) could be discussed and agreed as a group. Prior to the workshop, comprehensive notes on the use of NVivo were compiled by DMU and sent to case study authors.

The NVivo workshop proved to be a strong success, with most of the nodes for the case study analysis being created over the two-day period. However, following the workshop, there were technical problems with the software. This meant that some data held on NVivo was lost. This was very frustrating for the authors affected and led to information having to be re-input into the system. A further challenge was experienced among case study authors who were Apple users, because the software would not work on their devices. This was resolved by DMU providing PCs for use during the workshop. Following the workshop, Apple users had to borrow Windows computers for analysis of their interviews.



NVivo Nodes

4.2. Writing, Reviewing and Editing Drafts

Following the NVivo workshop, case study authors had 3 weeks to compile the first draft of their case study. This essentially involved pulling together background research and the interview to identify what the main ethical issues facing that particular organisation had been, and whether the interview had raised ethical issues which had not been identified in the literature.

Most case study authors were able to submit a first draft of their report by the first week of November. At this stage, each case study was returned to the interviewee for approval. This was not to ensure that the case study was seen as favourable to the interviewee or his/her organisation, but rather that the interviewee agreed on the content of the interview as presented. However, most interviewees were extremely busy and did not respond to the case study author. Given that the case studies had already received consent in advance of the interview, it was decided that interviewee confirmation of the case study was good to have but not essential, as it could have led to indefinite delays on the finalisation of each case study. However, it was also agreed to anonymise the interviewee unless there was a specific written consent by the interviewee to include their names in the final document.

Following its submission to UT, each case study was subject to peer review by two academics at the University. The peer review process looked at a number of issues, including quality of content, quality of English, and consistency of style across all of the case studies. When the case study had been reviewed it was returned to the author for appropriate edits. On occasion, it proved more time efficient for the peer reviewers to make stylistic changes themselves and for the author to confirm using track changes. The revised version was returned to UT by mid-December.

The QA process took place in January and performed the function of a third peer review by consortium partner the University of Central Lancashire, Cyprus, and highlighted further issues

which had not been recognised previously, drawing on the suggestions in D6.3 (Quality Assurance Plan). Once each case study had been reviewed by the QA process it was returned to its originating author for final edits before being sent on to the leader of WP 1.1 and the project coordinator. The leader of WP 1.1 then combined all of the case studies into a single deliverable (D1 .1) for submission to the European Commission by 31st January 2019, and the project coordinator conducted final edits before submitting them to the project workbook and the ORBIT Journal.

One unforeseen issue raised in early January was the inconsistency between the case studies and the QA criteria which had been introduced at the project launch in May 2018. A part of this was due to some of the case study authors not being at the launch event, but also from the QA leader not having been involved in the case study process. A Skype meeting was held to clarify the QA process, which raised a key question regarding the intended audience of the case studies. On the one hand, the intended audience was the European Commission, and through them practitioners who would be looking at the case studies as a means of understanding ethical issues within their own particular application domain. On the other hand, the case studies had been carried out in a rigorous manner such that they were suitable for publication in a social science journal. This meant that for each case study there were 2 intended audiences: academic and non-academic. It was decided that the focus of the case studies should be on the non-academic audience, with a more academic version later revised for publication in the ORBIT Journal.

5. Conclusion

A number of key challenges were faced in the design and development of the 10 case studies required for WP 1.1, but along with this quite a few lessons have been learnt. This concluding section will look first at the challenges faced and then lessons learnt, which should be taken as recommendations for future case study management and development.

5.1. Challenges

There were a number of challenges faced throughout the project. Underpinning many of these was the lack of experience of many of the case study authors. Of the 10 case studies, 6 were carried out by authors with little or no social science experience/background. This meant that many assumptions which could normally be made in the writing of case studies were not valid in this instance. This became particularly apparent during the QA process, which was the first time that the case studies had been reviewed by anyone with social science expertise.

A second challenge was the lack of time available to develop the case studies. It was agreed at an early stage that the case studies would be stronger with more interviewees. However, the realities of the time constraints provided with the work package meant that it was difficult to do this.

The third challenge was the time assigned to partners for writing the case studies. This averaged out at 1.85 PM per partner. For some partners, this proved to be too demanding, and there was some shuffling of PMs between partners to focus efforts on a handful of partners (e.g. UT leading 5 case studies).

A fourth challenge was that some partners dropped out of the process owing to red tape issues within their organisations. In yet other cases, no partners were found within the application domain at all. This was particularly true of the banking and securities sector, in which a case study had been envisioned to focus on the use of SIS in trading of securities.

Technical problems with the NVivo software formed a fifth challenge. As DMU migrated servers on which NVivo was hosted, crucial information was lost, leading to work having to be duplicated. Some of the information was regained from backup tapes, but sadly not all.

The sixth challenge was the focus on intended audience. The case studies had been conducted with a primarily academic audience in mind, with a view to the publication of the case studies in a special issue of an academic journal. However, the QA process was designed to make the case studies attractive and approachable for non-academics, and so included elements that an academic paper would not necessarily concern itself with, such as pictures, charts, and tables.

Table 9: Challenges

Challenge	Explanation
Experience	Lack of social science experience among some of the case study authors
Time	Lack of time for more interviews within organisations and additional organisations
Planning	Insufficient time allocated to some case study authors
Participation	Difficulty identifying, confirming, and liaising with case study participants
Technical	NVivo software crashing, incompatibility with Apple computers
Audience	Contradictory intended audiences

5.2. Lessons Learnt

Each of the aforementioned challenges can be used to highlight lessons learnt along the way. The first challenge was the lack of experience of case study authors in the social sciences. This is relatively easy to resolve, if one has social scientists available to conduct case studies. It is obviously preferable to use people with expertise in this area to develop such studies. In the absence of available resources, as was the case with the SHERPA project, it is crucial that assumptions are not made. The development of the case study protocol went a long way to resolve many of these issues. However, some topics were invariably missed from the case study protocol, such as interview technique and intended audience of the case studies themselves.

The second and third challenges to be faced was the time limit on the case studies, which meant that it was difficult to perform the case studies in much depth. More time would have allowed for a greater number of interviews, which in turn would have added richness to each case study. Once more, when using experienced social scientists this might be less of a problem than it was for the SHERPA project.

Problems with prospective partners dropping out needs to be factored into the risk analysis of any project. To account for this, more than the minimum number of case studies was conducted (we aimed for 11 case studies). This was vital to the success of the project, as one case study was dissolved by late December, still leaving us with the 10 required case studies.

While technical problems are unfortunately a staple of using software, the final challenges regarding the QA process and the intended audience could have been foreseen at an earlier stage in the process. The leader of the QA process could have been involved in the drafting of the case study protocol or attended at least one of the many weekly Skype meetings. She could have also

addressed her input during the monthly SHERPA partner meetings, or the project coordinator could have addressed the need for QA throughout the process. This would have ensured that the QA criteria was fully integrated into the case studies from an earlier stage.

5.3. Insights

The initial step of drafting the case study protocol went a long way to shaping expectations and providing consistency for the case studies. This consistency was aided further by the identification of a pilot case study at a very early stage in the process. Although this meant that the author of the pilot case study had to work harder than others in terms of keeping ahead of the pack, it did mean that consistency could be achieved more effectively.

The weekly case study Skype calls were also crucial to the successful completion of the case studies to a high standard within the time allotted. These are both provided a sense of team coherence and avoided case study authors feeling neglected or ignored. They also introduced an element of accountability on a regular basis which meant that few case studies fell behind, because each author knew that they had to give an account about their progress on a weekly basis.

The NVivo workshop at DMU was another notable success within the project. In conjunction with the weekly Skype calls, this led to the case study authors meeting in person for the first time as a group. It allowed for collective discussion on methodology and approach, and ensured that the majority of the case studies were all at a suitable point of progress by mid-October 2018.

Finally, the project leader was extremely supportive throughout the process of the development, writing, and reviewing of the case studies. Rather than being a distant figure, he attended a significant number of the weekly Skype calls, making himself available for clarification purposes. Furthermore, his leadership approach was one of encouragement and support, rather than attempting to be disciplinarian. He was understanding towards the partners with no social science experience and was very accommodating to reviewing the case studies, despite having a very busy schedule. This was very much appreciated by the case study authors and provided the effective guidance required for high-quality case study reports.

5.4 Next Steps

The case studies represent an important first step for the SHERPA project. They are the first visible publicly available deliverable of the project and support its claim to make an important contribution to the current debate around the ethics and human rights aspects of Smart Information Systems. It is therefore important for them to be visible and accessible through the various stakeholder groups with potential interest. They constitute their first set of major inputs into the SHERPA Workbook. It was therefore decided to publish the individual case studies in the workbook. At the same time each case study was submitted to and evaluated as a stand-alone paper of the ORBIT Journal. This was facilitated by the fact that the SHERPA coordinator simultaneously serves as the editor-in-chief of the ORBIT Journal. The ORBIT Journal is a platinum open access journal, i.e. it currently charges neither article processing fees nor any other fees to authors and is financially supported by the UK EPSRC-funded ORBIT project (www.orbit-rri.org).

The transfer of the case studies from this deliverable to the ORBIT journal required further review and revision. The eventual case studies that are published on the SHERPA website and workbook I therefore not always fully identical to the ones submitted in this deliverable. However, the quality of the published cases will be improved, due to at least one additional round of review.

In order to maximise attention and impact, the case studies are not publish simultaneously, but will be released individually during the first quarter of 2019.

6. References

Becker, J., Niehaves, B., 2007. Epistemological perspectives on IS research: a framework for analysing and systematizing epistemological assumptions. *Inf. Syst. J.* 17, 197–214.

Rowley, J., 2002. Using case studies in research. *Manag. Res. News* 25, 16–27.

Stake, R.E., 2005. Qualitative Case Studies, in: *The Sage Handbook of Qualitative Research*. SAGE Publications Ltd, Thousand Oaks, CA, pp. 443–466.

Walsham, G. (1995) 'Interpretive Case-Studies in IS Research - Nature and Method', *European Journal of Information Systems*, 4(2), 74-81.

Yin, R.K., 2015. *Qualitative research from start to finish*. Guildford publications.

Yin, R.K., 2003. *Case Study Research Design and Methods*, 3rd ed. SAGE Publications, UK.

Walsham, G. (1995) 'Interpretive Case-Studies in IS Research - Nature and Method', *European Journal of Information Systems*, 4(2), 74-81.

7. Appendices

7.1. Consent Form

Issue	Respondent's initials
I have read the information presented in the information letter about the case study	
I have had the opportunity to ask any questions related to this study, and received satisfactory answers to my questions, and any additional details I wanted.	
I am also aware that excerpts from the interview may be included in publications to come from this research. Quotations will be kept anonymous unless I give specific permission to the contrary (below).	
I give permission for my name to be associated with excerpts from the interview which may be included in publications to come from this research.	
I give permission for my organisation to be identified in any final publications produced by SHERPA.	
I give permission for the interview to be recorded using audio recording equipment. (if necessary).	

I understand that relevant sections of the data collected during the study may be looked at by individuals from or a project partner from SHERPA. I give permission for these individuals to have access to my responses.	
I understand that the audio recording may be given to a transcription service company to transcribe. I give permission for these organisations to have access to my audio files for transcription purposes	

With full knowledge of all foregoing, I agree to participate in this study.

I agree to being contacted again by the researchers if my responses give rise to interesting findings or cross references.

☐ No ☐ Yes

If yes, my preferred method of being contacted is:

☐ Telephone:

☐ Email:

☐ Other:

Participant Name		Consent taken by	
Participant Signature		Signature	
Date		Date	

7.2. Consent Form Information Sheet

SHERPA - Shaping the ethical dimensions of smart information systems (SIS) – a European perspective

Task 1.1 – Case Studies

Please take some time to read this information and ask questions if anything is unclear.

Contact details can be found at the end of this document.

What is the purpose of this study?

This study aims to develop a case study for the SHERPA project regarding ethical issues arising in the use of artificial intelligence and big data (Smart Information Systems - SIS). This information will be used to develop an analysis of these ethical issues and, thereafter, a workbook on the responsible development of SIS. The information gained from these interviews will identify potential gaps in understanding and reinforce comprehension of well-known issues.

Who is organising this research?

The research for this study is being undertaken by

A Research Ethics Committee has reviewed and approved this research.

Why have I been chosen?

The project aims to develop 10 case studies from a number of different contexts. These will include business, government, insurance, agriculture and banking. The aim is to develop a broad understanding of ethical issues spanning these contexts, recognizing similarities and differences. You have been chosen as a member of one of these contexts with a good understanding of the use of SIS within your own particular context.

Do I have to take part?

Participation in this study is voluntary and you may ask any questions before agreeing to participate. If you agree to participate, you will be asked to sign a consent form. However, at any time, you are free to withdraw from the study and if you choose to withdraw, we will not ask you to give any reasons.

What will happen to me if I take part?

If you agree to take part in this study we will interview you in person, or by phone/Skype, regarding your experience with SIS.

We may ask you to participate in a follow-up interview, though participation in this is optional.

What are the possible benefits of participating?

The study aims to develop an understanding of ethical issues, the purpose of which is to inform the SHERPA project proposals for the responsible development of SIS. In addition to helping the SHERPA project, advanced ethical analysis will be carried out on the case study to which you contribute, which may raise issues that your organisation would like to know about and take steps to remedy.

What are the possible risks of taking part?

There are no risks in taking part in this study. At any time during the interview you can choose to withdraw. You may also choose to withdraw your data from being used in the project at any time until 1 January 2019.

How will my interview be used?

The case studies will combine quantitative and qualitative elements and will be designed and analysed by SHERPA project partners who have experience in ethical analysis. The recording of the interview may be transcribed by parties outside of the consortium. If this happens, the transcription company will delete the recording and transcription after the transcription is approved. On the consent form we will ask you to confirm that you are happy for the SHERPA consortium to use and quote from your interview. Any such use will be anonymous unless you indicate otherwise on the

consent form. Information which will identify your organisation will also be kept out of publications unless otherwise indicated on the consent form.

What will happen to the results of the project?

All the information that we collect about you during the course of the research will be kept strictly confidential. You will not be identified in any reports or publications and your name and other personal information will be anonymised unless you indicate otherwise on the consent form.

What happens to the interviews collected during the study?

The interviews will be transcribed by the interviewers or a designated, approved third-party agency. If we use a third-party transcription service, we will ensure that there is a signed data processing agreement in place. The audio files will be deleted, once the analysis of the interview is complete.

What happens at the end of the project?

You may request a summary of the research findings by contacting Kevin Macnish, University of Twente (k.macnish@utwente.nl).

What about use of the data in future research?

If you agree to participate in this project, the research may be used by other researchers and regulatory authorities for future research.

Who is funding the research?

This research is funded by the European Commission] under grant no. 786641.

What should I do if I have any concerns or complaints?

If you have any concerns about the project, please speak to the researcher, who should acknowledge your concerns within ten (10) working days and give you an indication of how your concern will be addressed. If you remain unhappy or wish to make a formal complaint, please contact Kevin Macnish, k.macnish@utwente.nl.

Fair Processing Statement

This information which you supply and that which may be collected a part of the project will be entered into a filing system or database and will only be accessed by the researcher and supervisor involved in the project. The information will be retained by the researcher's institution and will only be used for the purpose of research, statistical and audit and possibly commercial purposes. By supplying this information you are consenting to us storing your information for the purposes above. The information will be processed by use in accordance with the provisions of the Data Protection Act 1998. No identifiable data will be published.

7.3. Template for Final Report

Length: 7500 - 9000 words

Structure:

1. Introduction – 300 - 500 words

Introduce

- A. The topic and describe the aim of the report
- B. Any case-specific research question(s),
- C. Methods (to the extent different from the general approach advocated for the case studies) and
- D. Outline of the remainder of the report.

2. Background review: ethical issues in the application domain you are discussing (e.g. SIS in health care) – 1500 - 2500 words

(Literature review)

- A. Description of the domain and its use of SIS (i.e. how SIS is currently being used in healthcare)
- B. Survey of ethics literature of SIS in the domain you will discuss, as well as own identification of ethical issues [Do this in a systematic way that gives an overview of ethical issues that have been identified and discusses each]
- C. Conclusion

3. Introduction to the case study and descriptive analysis – 2000 – 2500 words

(Empirical research, interviews, literature study presented in journalistic style)

Description of the setting:

- A. description of the organisation(s) and individual(s) interviewed - interview questions 1-6,
- B. of the SIS systems(s) being used by the organization(s) - interview question 7,
- C. the aims of the organization(s) in using these systems - interview question 8,
- D. does the system work as intended or are there issues with its operation - interview question 9,
- E. identify some general (non-ethical) impacts that the system has (had) on the organization - interview questions 10-12.
- F. the way in which the system(s) work - interview questions 13-14,
- G. the policies governing the system(s) use - interview questions 15-16,
- H. who are stakeholders and what is the impact on them - interview questions 17-24

4. Ethical issues – 2000 – 2500 words

- A. Identify benefits and harms of the system from the point of view of stakeholders.
- B. Identify ethical issues with the system(s),
 - a. That are the result of the design and normal operation of the system, and
 - b. The particular uses and responses to it or its impact by stakeholders. (These can be ethical issues recognized by stakeholders or not recognized.)
- c. Discuss the extent to which these are recognized by stakeholders and any remedial measures that have been taken already (laws, policies, initiatives, redesigns, etc.).
- d. Draw upon the information gathered during the interviews; literature study; and research about the case

5. Conclusion 500 – 1000 words

Summary of findings.

- A. What have we learned from the case study?
- B. What are possible ways in which the ethical issues can be mitigated?
- C. What further investigations should be done?

8. The Case Studies

CS01 – Employee Monitoring and Administration



Case Study: The Internet of Things and Ethics



This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641

Document Control

Deliverable	D1.1 Case Studies
WP/Task Related	WP1 Representation and Visualisation of ethical and human rights issues in SIS
Delivery Date	M9
Dissemination Level	Public
Lead Partner	UT
Contributors	UCLanCY, Josephina Antoniou AHR, Andreas Andreou
Reviewers	
Abstract	
Key Words	

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes
0.1	08/11/2018	Josephina Antoniou, Andreas Andreou	The report has been reviewed by the interviewees in the spirit of responsible research	First Submitted Draft of the IoT Case Study Report, Lead Partner: UCLan Cyprus, Other Partners: AEQUITAS Human Rights
0.2	22/01/2019	Josephina Antoniou, Andreas Andreou		Adopting suggestions and edits and prepare an updated version

Contents

Executive Summary	33
1. Internet of Things and Ethics: A Case Study	34
1.1 Business Use of IoT for Surveillance	34
2. Background Review	36
2.1 Legal Issues: Employee Monitoring and Asset Tracking	36
2.1.1 Legal / Human rights analysis	38
2.1.2 Jurisprudential Analysis	40
2.2 Monitoring, privacy and consent – Is consent a panacea?	41
2.3 Monitoring and tracking – Ethical, economic and legal dimension	42
2.4 A comparative approach: US, China, Canada and Europe	42
2.5 Overall Conclusions of Background Review	43
3. CRM.COM	44
3.1. Description of the Organisation and Individuals	44
3.2. Description of SIS Technologies Being Used	44
3.3. The Aims of the Organisation Designing This Technology	45
3.4. Limitations and Constraints of Using this Technology	45
3.5. Types of Data Used	46
3.6. Policies Governing the Use of SIS Technology	46
3.7. The Effects on Stakeholders	47
4. Ethical Issues	47
4.1. Access to SIS	48
4.2. Discrimination and Inequality	49
4.3. Informed Consent	49
4.4 Potential for malicious use	50
4.6. Privacy	50
4.8 Transparency and Trust	52
5. Conclusion	52
5.1 Limitations	53
5.2 Contribution to knowledge	54
5.3 Implications of this report	54
5.4 Further Research	54
6. References	54

Executive Summary

The Internet of Things (IoT) may be defined as a network of networks, where the end devices are not user-handled devices but can be computing devices, mechanical and digital machines. In many businesses, IoT-based software is used increasingly as a means to deliver enhanced customer service and improved business management procedures. By using IoT to monitor business operations, through tracking-capable software, businesses are, for instance, able to track products and employees. The issue is further explored in the literature review (Section 2).

Section 2 starts by offering some general remarks about the topic under discussion (Internet of Things – hereinafter IoT – and monitoring employees) including the harm that occurs. Then, section 2.1.1. is dedicated to the legal/human rights analysis as it is presented through the literature. In this section, an account on suggestions for Guidelines and policies on monitoring is offered. Part 2.1.2 is a jurisprudential analysis and it contains information about important case law, again, as presented through the literature. This part emphasises the importance of the jurisprudence of the European Court of Human Rights. The issue of consent is presented in section 2.2, where it is argued that it is not a panacea. Section 2.3 is about the ethics and perceptions around monitoring and tracking. Section 2.4 gives information about comparative literature on monitoring and employee privacy, followed by some concluding remarks.

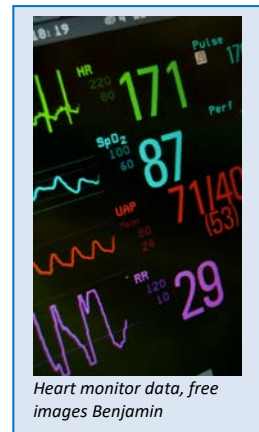
1. Internet of Things and Ethics: A Case Study

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

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

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

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



The use of the IoT can be associated with the generation and manipulation of vast amounts of data that may relate to human behaviour and interaction, popularly known as Big Data. Big Data and its manipulation can result in potentially high impact, for instance, on privacy, security and consumer welfare (Kshetri 2014). This is particularly so as the process of data collection in IoT is done automatically, often without any human intervention.

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

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

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

1.1 Business Use of IoT for Surveillance

In business, IoT proved to be a solution for saving time and money, for improving the customer experience and employee productivity, and for overall monitoring business processes. In fact, asset-

tracking and monitoring are thought to be a driver for business innovation (Tournier, 2017). Following the developments in technology, according to Karahisar (2014), *monitoring* has steadily increased in several types of environments such as educational institutions, roads, subway transportations, as well as in people's habitats, (predominantly in urban settings). The same applies in the workplace. Due to the increase in *cyberloafing*¹³ and consequent lawsuits, employee monitoring has become more widespread and much easier with the use of new and cheaper technologies (Mujtaba, 2004). In fact, nearly 80% of organizations use some type of electronic performance tracking (Tomczak, Lanzo and Aguinis, 2018); estimates indicate that over 26 million workers are electronically monitored (G. Stoney, 1998).

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

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

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



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

¹³ This is a term often used to describe the habit of employees to use their Internet access for personal use.

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

This will be done by analysing key issues within the literature and current legislation on the topic and by conducting interviews with two software designers working for an international company, which develops and markets *on-demand and on-premise software for Subscription Billing and Rewards, which uses IoT* – CRM.COM (crm.com, 2017). The case study further aims to identify whether software development and distribution organisations face ethical issues in IoT usage in practice, and further, if there are policies and procedures set in place for addressing these concerns; and whether they face additional issues not addressed in the literature.

This case study will first review the current literature and legislation relevant to such activities as monitoring and tracking, as well as using IoT technologies (Section 2), and thereafter present CRM.COM focusing on how it provides tracking software as a service and as a product for businesses nationally and in several countries worldwide (Section 3). Finally, the case study will discuss the ethics of such IoT-powered software products, by considering both their design and their usage (Section 4).

2. Background Review

The background review focuses on the effects of monitoring and tracking from a legal and ethical perspective and what aspects need to be considered as the study moves on to investigate the effects of a selected SIS that is used for such purposes, given the legal groundwork outlined next. This section, therefore begins with the legislation of employee monitoring and asset tracking, presenting both a legislative analysis and a jurisprudential analysis. The section then moves on to discuss specific cases of privacy and discrimination as related to monitoring. The section closes with an overview of the ethics of monitoring and tracking as highlighted in important publications.

Given that employee monitoring and asset tracking is not a new topic, there are a few cases to discuss. However, the application of these practices with the use of SIS is a recent development, which accounts for the lack of legislative analysis so far.

2.1 Legal Issues: Employee Monitoring and Asset Tracking

The report starts by offering some general remarks about the topic under discussion (Internet of Things – hereinafter IoT – and monitoring employees) including the harm that occurs. Then part 2.1.1. is dedicated to the legal/human rights analysis as it is presented through the literature. In this part, an account on suggestions for Guidelines and policies on monitoring is offered. Part 2.1.2 is a jurisprudential analysis and it contains information about important case law, again, as presented through the literature. This part emphasises the importance of the jurisprudence of the European

Court of Human Rights. The issue of consent is presented in part 2.2, where it is argued that it is not a panacea. Part 2.3 is about the ethics and perceptions around monitoring and tracking. Part 2.4 gives information about comparative literature on monitoring and employee privacy. The paper finishes with concluding remarks.

The use of monitoring technologies in the workplace and its many forms

The use of monitoring technologies in the workplace is a topic which received attention from scholars and it has been addressed and touched upon from various angles.

In the Internet age, as Frayer argues in his article *Employee privacy and Internet monitoring: Balancing workers' rights and dignity with legitimate management interests* (E. Frayer, 2002), employers face serious risks from employee misuse of the new communication medium (referring to emails). In fact, the tendency of employees to misuse the internet at their workplace is also confirmed through employees' testimonies in the article *Ethical Implications of Employee Monitoring: What Leaders Should Consider*, by Mujtaba (2004). Moreover, Martin and Freeman (2003) – their article will also be mentioned below – hold that in 2001, 60.7% of employees surveyed said they visit Web sites or surf for personal use at work.

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

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

The harm

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

surveillance results in workers feeling humiliated, and may lead to stress, demoralization, and stress-related health problems in workers. Her article is based on desktop research.

Relevant to the ethical and legal dimension of the phenomenon is Karahisar's stance, that the case of constantly being monitored and tracked has led to the established opinion from employees that there is no privacy at work. In a similar framework, Frayer mentions that employee advocates assert that such surreptitious monitoring may infringe on employee privacy and other protected workplace rights. The feeling of invasion of the privacy of the employees is also mentioned in the article *Ethical Implications of Employee Monitoring: What Leaders Should Consider*, written by Mujtaba (2004). The issue of privacy, which is strongly connected to the IoT, is indeed important and it is also extrapolated in other articles – such as *Employee monitoring: Privacy in the workplace?* by Mishra and Crampton (1998).

Beyond Karahisar, the authors of *Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses*, Chory, Vela and Avtgis (2016), examine concerns on privacy rights, due process, and fairness through an empirical study of full-time working adults' beliefs through an empirical study of full-time working adults' beliefs about their computer-mediated workplace communication privacy and their evaluations of organizational justice, trust in upper management, and commitment to the organization. Their results suggest that employees who do not perceive much privacy, tend to view their organization's policies as less fair, trust upper management less, and demonstrate less commitment to their organizations.

In *Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives* (Alder, (1998)), it is demonstrated through desktop research that monitoring is seen by some as dehumanizing, that it invades worker privacy, increases stress and worsens health, and that it also decreases work-life quality.

What was discussed so far shows that the IoT can be harmful. In particular the use of monitoring technologies in the workplace, which is a widespread practice that takes many forms, causes harm. In fact, monitoring employees has multidimensional effects not only on employees (their human rights, their health (including psychological), and their general well-being) and on ethics and human rights in general, but also on the business itself as it affects the way in which employees perceive their professional environment, something which can be said that it affects the performance. For example, they 'demonstrate less commitment to their organizations' as already mentioned).

2.1.1 Legal / Human rights analysis

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

Guidelines and policies on monitoring

Since monitoring is a practice which can result in a violation of rights, the need for guidelines and policies on monitoring are mentioned in some articles. For example, in *Employee monitoring: Privacy in the workplace?* Mishra and Crampton, (1998) discuss the fact that employers can defuse or avoid the negative effects of monitoring, by following certain guidelines. What is more, the authors maintain that employers should undertake such activities with much forethought and care. In *Balancing Employer Monitoring and Employee Privacy*, Mohl (2006) seems to agree as he argues that '*regardless of what form of monitoring an employer utilizes, care must be taken to ensure that it does not violate employees' privacy rights.*'

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

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



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

In the same framework, the *Bărbulescu v. Romania* case of the ECtHR reaffirms the importance of having full policies setting out in clear terms the circumstances in which personal use of systems is permitted as well as the extent of monitoring and circumstances in which it may occur.

In *Ethical Implications of Employee Monitoring: What Leaders Should Consider*, by Mujtaba (2004), which looks at cyber loafing, the author mentions actual samples of employees' perceptions and feelings from the surveys and discussions on having their Internet use at work being monitored. The majority of the respondents seem to be at ease with monitoring and to understand the reasons of its existence. For example:

'I have no problem with my work monitoring my internet use, [...] because it can be a money saving tool to weed out the cyber loafers' said one respondent while another one said that 'I expect to be monitored in my organisation. The job I have requires full secret national security clearance. The data is sensitive and restricted. My company would be foolish not to institute security measures. The data of my company and its subcontractors and the governments cannot be compromised. Therefore, everyone here is aware of the consequences of downloading prohibited content or surfing excessively'. A third respondent expressed the view that 'Unfortunately, many individuals abuse their right to the Internet and play around when they should be performing valuable work for their

organisation. So, monitoring policies/guidelines should be developed and communicated'. Another responded said that '[...] So, I am aware that my incoming and outgoing emails and Internet connections are being monitored by the company. I am OK with this policy as I am aware of it. [...]'. However, this responded adds that 'Respecting a worker's basic privacy and essential needs, an employer could include provisions for private use of Internet in the policy. I really don't like the idea of being monitored. But most people don't mind being accountable to somebody. They don't mind being monitored as long as they know about it'. A worker who also expressed that they do not like being monitored, said that 'personally I really do not like the idea of being monitored. It's an issue of privacy and having personal space at work'. Relevant to that argument is another worker's view that the line between personal and professional Internet usage is blurred.

2.1.2 Jurisprudential Analysis

The jurisprudence on monitoring employees has its own place in the academic literature. In this part of the paper, five papers are presented, which present and analyse important cases from the United Kingdom, Romania and Israel.

United Kingdom: The recent case of *McGowan v Scottish Water* demonstrated the issues related to employee monitoring in practice. An employee claimed unfair dismissal, but his employer argued he had been forging his timesheets. The employer had carried out covert video surveillance of the employee's home to get evidence of when the employee left for and returned from work and then compared those times with his timesheets. The issue in the tribunal was whether the video evidence breached the Human Rights Act 1998 because it had been obtained covertly and, therefore, ignored the respect for the employee's privacy. The tribunal held that the surveillance operation was not disproportionate to the circumstances and was undertaken to protect the employer's assets.

Therefore, the video was accepted as evidence. (Legal Q & A: Employee monitoring, Personnel Today 18, 2006)

*Employee privacy
versus protection of
employer assets.*



Romania: *Bărbulescu* case is examined in the *European Court of Human Rights: Monitoring Employee Communications Ruled Unlawful* (Temperton and Illing, 2017). In this case, Bărbulescu challenged his employer in the Romanian courts and later at the European Court of Human Rights (ECtHR), alleging a breach of *Article 8 of the European Convention on Human Rights* (the right to respect for private and family life, home and correspondence). The authors hold the view that the 'ruling (of the ECtHR) appeared to set the bar quite low on the facts' as 'an employer did not seem to have to establish a particularly compelling reason to monitor in order for the proportionality requirements to be met'. The case was referred to the Grand Chamber of the ECtHR. The authors are not surprised by the new decision and they hold that the Grand Chamber puts the bar back where it should have been – the employer needed to do more in order to meet the tests that would justify monitoring. They also believe that an important reason why the applicant's arguments succeeded was the fact that his employer was not clear about the nature and extent of any monitoring.

Barbulescu v Romania is indeed a very interesting case, and as is discussed in *Workplace Monitoring and the Right to Private Life at Work* (Atkinson 2018), it clarified the application of Article 8 (right to private life in the workplace), and the extent of the state's positive obligations to protect the right against workplace monitoring. In his analysis, Atkinson also supports that the decision establishes the

fact that there is an irreducible core to the right to private life at work that does not depend on an employee's reasonable expectations of privacy, and sets out clear principles for striking a fair balance between Article 8 and the employer's interests in the context of workplace monitoring.

Israel: Mirchin (2012), in his article 'Monitoring Employee Online Activity', he discusses a recent landmark National Labour Court (NLC) decision in Israel, which established principles that specify how employee emails and computer usage can be monitored. The article explains that the decision, which held that monitoring/inspecting personal email constitutes a significant invasion of privacy and thus it should only be permitted under specific circumstances, weighed heavily in favour of employees, significantly increasing their privacy rights. As a result, employers in Israel are now more careful about monitoring employees' online activity unless certain circumstances exist, while they are avoiding policies that are generic or vague for email and computer use. Among the established principles are: maintain a clear email policy, evaluate less invasive alternatives for monitoring employees, and obtain employees informed and written consent to the monitoring activity.

A decision in Israel weight heavily in favour of employees' privacy.



The importance of the jurisprudence of the European Court of Human Rights

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

The above demonstrates that there is there are different proposals and approaches to the issue if monitoring employees, which can help us extract ideas and conclusions for the wider landscape of the IoT.

2.2 Monitoring, privacy and consent – Is consent a panacea?

The recent Regulation on General Data Protection (GDPR) (2018) and its practice in Europe, makes it clear that for any employee monitoring to take place (and hence for any personal data to be collected), consent must be given by the employee. However, even with the existence of legally compliant practices such as signed consent forms, unethical practices might do take place. For example, Macnish (2018) discusses the fact that that, even though the seeking of consent between two parties

demonstrates mutual respect, reinforces autonomy and generally assures fairness, often this is not the case, since there are at least three ways in which consensual transactions might be invalidated, and they include fraud, exploitation and coercion.

This shows that informed consent cannot be seen as a panacea.

2.3 Monitoring and tracking – Ethical, economic and legal dimension

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

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

In *Surveillance in Employment: The Case of Teleworking* (1999), Fairweather argues that while employers have a legitimate interest in a certain amount of monitoring of their employees, an employee is not a slave. Hence, an employee should not be required to reveal their whole self to the employer but instead has a right to privacy. Fairweather argues that to allow intimate information to remain private, workers and

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

teleworkers should not normally have personal communications under surveillance by their employer, and the employer should not routinely monitor the nature or content of a worker's home life.

2.4 A comparative approach: US, China, Canada and Europe

Different legal systems and traditions have different approach to the issue of monitoring and privacy. The authors of the article *Intrusive monitoring: employee privacy expectations are reasonable in Europe, destroyed in the United States*, Determann and Sprague (2011), observe that many historic differences in the workplace are levelled by globalization but there is still a very big difference on the law on workplace privacy, between the United States and the European Union. They believe that this difference raises challenges for employers who manages and monitors worldwide human resources with global processes and technologies. Due to this challenging reality, the authors examine the contrasting policy and legal frameworks relating to data privacy in the US and the European Union, with a particular focus on workplace privacy and intrusive surveillance technologies and practices. The authors argue that in general, the right to privacy in the US is conditioned on a reasonable expectation of privacy.



In *Monitoring employee activity without infringing privacy laws*, Cheng, Liu and Jiang (2010) argue that the legal framework relating to individual privacy and data protection in China is rather patchy and incomplete and that there is currently no set of laws or regulations that specifically address data privacy or protection in the context of employment.

Overall, conclusions for the approach towards the regulation of employee monitoring and asset tracking is elaborated in *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada* (Lasprogata, King and Pillay, 2004), which discusses among others the right to privacy in a comparative way between the USA, Canada, and the EU. The article dedicates a large part on discussing the regulation of electronic monitoring of employees in the USA, Canada, and the EU. The authors hold that relevant laws in monitoring exist in a context that recognizes the valid business reasons for electronic monitoring and considers the interests of employees in workplace privacy and, 'in this respect the EU, United States, and Canadian approaches are similar; all give some due to the business reasons for electronic monitoring'. However, there are radically different approaches between the EU, Canada, and the United States in regards to regulating electronic monitoring. The authors also claim that a comparison between the relevant laws in these geographies 'fails to reveal a common legal paradigm for multinational employers that would support a uniform electronic monitoring policy for all employees working in these countries'. They go on to support that 'The lack of a common legal paradigm for the EU, Canada, and the United States is due to inconsistencies in the privacy laws and underlying value systems of the different countries, and the variety of factors that alter the lawfulness of employee electronic monitoring from country to country'.

2.5 Overall Conclusions of Background Review

Throughout this background research into, mainly the ethical and legal issues of using Smart Information Systems (SIS), it becomes clear that up to now, the issue is approached more from the perspective of monitoring people. However, there is the issue of asset tracking (tracking our physical belongings, through, for example, barcode scanning, or GPS), which is more subtle but can still manipulate personal or sensitive data and support unethical practices, if not addressed early on. Both monitoring and tracking within a business have been, undoubtedly, fundamentally affected by the development and use of SIS technology (for example, IoT) and electronic communications in the workplace. The main conclusion that can be drawn from the literature review is that there are a plethora of concerns with regards to human rights violations of employees – in particular, the right to privacy – and ethical principles. There are also many legal principles, laws and jurisprudence, which address some of these issues. Alder (1998) remarks that there are opposing opinions regarding workforce tracking and electronic performance monitoring and that both proponents and opponents of electronic monitoring fail to adequately address the arguments voiced against their point of view.

A more specific, thoroughly considered and, ideally, legally binding strategy/set of rules must be created, which will allow safeguarding employers' benefits, without violating employees' rights and needs. The need for monitoring can be totally understood and accepted, but as an employee said and was mentioned above, the line between personal and professional Internet usage is blurred. Thus, it is important to take into consideration what employees legitimately feel (mentioned above are, among others: 'respecting a worker's basic privacy and essential needs' and 'It's an issue of privacy and having personal space at work') and find a balanced solution among the interests of employers

and the rights and needs of employees. The literature mentioned in this review can be proven useful for finding ideas for guidelines and ideas.

3. CRM.COM

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

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

3.1. Description of the Organisation and Individuals

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

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

3.2. Description of SIS Technologies Being Used

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

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

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

Second, the software can be offered as a stand-alone solution, where the software is installed at the customer's site, and thus, the customer has complete control over the management and use of the

software, unless otherwise decided by the customer. In this case, even if CRM.COM supports the customer with maintenance tasks, they cannot control the software usage.

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

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

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

‘the information that we track is information that was going to be shared with the company anyway; [...] in order for the company to bill it’, (George Rossides)

and clarified that they

‘do not track information that is not immediately needed or information that is sensitive.’ (Panayiota Demou)

3.3. The Aims of the Organisation Designing This Technology

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

‘store it on their own server, then we do not have control over it.’ (George Rossides)

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

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

3.4. Limitations and Constraints of Using this Technology

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

‘The past year we have studied the GDPR regulation in depth and we introduced several features in order to encourage our clients to comply with the regulation’. (Panayiota Demou)

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

3.5. Types of Data Used

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

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

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

‘preferences of a customer, personal information of the customer or information related with the behaviour of the customer’. (George Rossides)



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

3.6. Policies Governing the Use of SIS Technology

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

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

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

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

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

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

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

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

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

3.7. The Effects on Stakeholders

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

'We always provide support unless the customers request otherwise. It's the nature of our business'. (Panayiota Demou)

The main customers come from:

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

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

'all around the world'. (George Rossides)

4. Ethical Issues

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

These ethical issues have in large part been discussed in the interviews, matching in several cases issues highlighted by literature and legislation. Interview questions have been informed by literature

and legislation in that respect. The main issues discussed include the ethics of access to the IoT-based software, issues of discrimination and equality that may arise from the use of the IoT-based software, the importance of informed consent, the potential of malicious use, issues of privacy, responsibility, as well as transparency and trust with a reference to the use of personal data by the SIS.

Figure 1 – Ethical issues in IoT-Based Tracking



4.1. Access to SIS

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

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

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

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

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

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

4.2. Discrimination and Inequality

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

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

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

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

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

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

4.3. Informed Consent

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

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

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

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

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

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

4.4 Potential for malicious use

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

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

However, there is no official policy to address such behaviour. The actions that will be taken in case malicious use of the system is detected, varies:

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

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

‘breach of personal data, malicious software coming into your personal device... those kind of things’. (Panayiota Demou)

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

‘All the information which is exchanged between the systems is encrypted’. (George Rossides)

4.6. Privacy

IoT is by its very nature susceptible to privacy breaches as it has been used in businesses to monitor

and track users and their environment, without the need for human intervention. According to the interviewees,

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

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

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

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

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

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

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

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

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

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

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

From the narrative above, we have already identified that according to the interviewees, in addition to data necessary for billing, e.g. asset's consumption, the only items of personal data collected are IDs and Passwords for identification purposes, although all data is anonymised prior to being stored.

The names are retrievable, though, through a process known as pseudonymisation, which allows the original data to be retrievable upon request:

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

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

4.8 Transparency and Trust

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

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

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

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

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

The customers can of course stop this:

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

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

5. Conclusion

This IoT case study introduced an IoT-powered software for asset tracking, a process that requires live data collection including personal data. The software design process in this case requires to consider

relevant legislation, responsibility issues and delivery and support of software. Despite the attempts made within the software design and development phases to incorporate as many features as possible to promote the software's ethical and responsible use, there are still a number of ethical issues that need to be addressed when the IoT SIS technology is used by its users, e.g. privacy, transparency and trust; often businesses themselves (e.g. retail or technology businesses) that can use it to track their own customers and employees.

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

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

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

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

5.1 Limitations

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

Another limitation is that the administrators of the software in case of standalone installations on local servers can solely control access to the system. The administrators, in this case, are employees of the customer businesses and the company that developed the software has no monitoring access to the logs unless given by the administrators. The administrators also can assign permissions to the use of the software at their own discretion. To avoid using the software according to the discretion of each user, appropriate policies and/or employee training could overcome the specific limitation.

5.2 Contribution to knowledge

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

5.3 Implications of this report

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

5.4 Further Research

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

6. References

- Alder, G. S. (1998). *Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives*, Springer Business Ethics, 7 (17), pp. 729 – 743.
- Alvino, I. (2016). New limits to the remote monitoring of workers' activities at the intersection between the rules of the Statute and the privacy Code. *Labour & Law Issues*, 2(1), pp.1-45.

- Atkinson, J. (2018). Workplace Monitoring and the Right to Private Life at Work. *The Modern Law Review*, 81(4), pp.688-700.
- Cheng, P., Liu, D. and Jiang, C. (2010). Monitoring employee activity without infringing privacy laws. *China Staff*, 16(1), pp.24-27.
- Chory, R., Vela, L. and Avtgis, T. (2016). Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses. *Employee Responsibilities and Rights Journal*, 28(1), pp.23-43.
- Crm.com. (2017). *Who We Are*. [online] Available at: <http://www.crm.com/company/who-we-are> [Accessed 2 Nov. 2018].
- Determann, L. and Sprague, R. (2011). Intrusive monitoring: employee privacy expectations are reasonable in Europe, destroyed in the United States. *Berkley Technology Law Journal*, [online] 26(2), pp.979-1036. Available at: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1899&context=btlj> [Accessed 2 Nov. 2018].
- E. Frayer, C. (2002). Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests. *The Business Lawyer*, [online] 57(2), pp.857-874. Available at: <https://www.jstor.org/stable/40688047> [Accessed 2 Nov. 2018].
- Edwards, G. (2015). Employee Monitoring. What are the Legal Issues?. *Credit Management*, p.49.
- Fairweather, N., B. (1999). Surveillance in Employment: the Case of Teleworking, *Journal of Business Ethics*, 22(1). Pp. 39-49.
- G. Stoney, A. (1998). Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives. *Journal of Business Ethics*, [online] 17(7), pp.729-743. Available at: <https://link.springer.com/article/10.1023/A:1005776615072> [Accessed 5 Nov. 2018].
- Gorman, J. (1998). Monitoring Employee Internet Usage. *Business Ethics: A European Review*, 7(1), pp.21-24.
- HR Focus (2013). High-Tech Tracking: Good Business Practice or Orwellian Nightmare? May 2013, 90(5).
- Hugl, U. (2013). Workplace surveillance: examining current instruments, limitations and legal background issues. *Tourism & Management Studies*, [online] 9(1), pp.58-63. Available at: <http://www.scielo.mec.pt/pdf/tms/v9n1/v9n1a09.pdf> [Accessed 6 Nov. 2018].
- Karahisar, T. (2014). Developments in Communication Technologies and Employee Privacy in the Workplace. *Journal of Media Critiques*, 1(3), pp.221-234.
- Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, 38(11), 1134-1145. doi: 10.1016/j.telpol.2014.10.002
- LASPROGATA, G., J. KING, N. and Pillay, S. (2004). Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada. *Stanford Technology Law Review*, [online] 4. Available at: <https://www.sukanyapillay.com/wp-content/uploads/Regulation-of-Electronic-Employee-Monitoring.pdf> [Accessed 1 Nov. 2018].

- López, R. and Schwarz, R. (2017). Corporate monitoring by technological means in Spain: overview of substantive and procedural conceptual construction. *JURIS - Revista da Faculdade de Direito*, 27(1), pp.11-48.
- Madakam S, Ramaswamy R, Tripathi S (2015) *Journal of Computer and Communications*, 3, 164-173, at: https://file.scirp.org/pdf/JCC_2015052516013923.pdf
- Macnish, K. (2018) *The Ethics of Surveillance: an introduction*. Routledge: London.
- Macnish, K. (2015). An Eye for an Eye: Proportionality and Surveillance, *Ethical Theory and Moral Practice* 18, no. 3 (2015): 529–48, doi:10.1007/s10677-014-9537-5.
- Martin, K. and Freeman, R. (2003). Some Problems with Employee Monitoring. *SSRN Electronic Journal*, 43(4), pp.353-361.
- Miedema, A. and Pushalik, A. (2009). *How, and when, employers should monitor employees*. [online] Hrreporter.com. Available at: <https://www.hrreporter.com/article/7295-how-and-when-employers-should-monitor-employees/> [Accessed 6 Nov. 2018].
- Mirchin, D. (2012). Monitoring Employee Online Activity. *Information Today*, 29(2), pp.32-33.
- Mishra, J. and Crampton, S. (1998). Employee monitoring: Privacy in the workplace?. *Advanced Management Journal*, [online] 63(3), pp.4-14. Available at: http://faculty.bus.olemiss.edu/breithel/final%20backup%20of%20bus620%20summer%202000%20from%20mba%20server/frankie_gulledge/employee_workplace_monitoring/employee_monitoring_privacy_in_the_workplace.htm [Accessed 4 Nov. 2018].
- Mohl, D. (2006). Balancing Employer Monitoring and Employee Privacy. *Workspan*, pp.68-70.
- Moore, A. (2000). Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy. *Business Ethics Quarterly*, 10(3), pp.697-709.
- Mujtaba, B. (2004). Ethical Implications of Employee Monitoring: What Leaders Should Consider' *Journal of Applied Management and Entrepreneurship*. *The Journal of Applied Management and Entrepreneurship*, 8(3), pp.22-47.
- Personnel Today. (2006). *Employee monitoring - Personnel Today*. [online] Available at: <https://www.personneltoday.com/hr/employee-monitoring/> [Accessed 6 Nov. 2018].
- Sychenko, E. (2017). International Protection of Employee's Privacy under the European Convention on Human Rights. *Zbornik Pravnog Fakulteta u Zagrebu*, 67(5), pp.757-781.
- Tomczak, D., Lanzo, L. and Aguinis, H. (2018). Evidence-based recommendations for employee performance monitoring. *Business Horizons*, 61(2), pp.251-259.
- Tournier, B. (2017). *IoT-Enabled Asset Tracking is Driving Business Innovation*. [online] Sierrawireless.com. Available at: https://www.sierrawireless.com/iot-blog/iot-blog/2017/09/iot_enabled_asset_tracking_is_driving_business_innovation/ [Accessed 8 Nov. 2018].
- Yerby, J., (2013). Legal and Ethical Issues of Employee Monitoring, *Online Journal of Applied Knowledge Management*, 1(2), pp. 1 – 55.

CS02 – Government



Ethics of Public Use of AI and Big Data: The Case of Amsterdam's Crowdedness Project



**This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641**



Document Control

Deliverable	Deliverable 1.1: Case Studies
WP/Task Related	WP1: Representation and Visualisation
Delivery Date	31/1/2019
Dissemination Level	Public
Lead Partner	University of Twente
Contributors	Mark Ryan, University of Twente
Reviewers	Kevin Macnish, Bernd Stahl, Doris Schroeder
Abstract	
Key Words	

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes
0.1	19/11/2018	Mark Ryan	Kevin Macnish	
0.2	03/12/2018	Mark Ryan	Kevin Macnish	
0.3	07/01/2019	Doris Schroeder		Editing, adding elements, commentary, QA

Contents

Executive Summary	60
Government, Smart Information Systems, and Ethics	61
1. The Use of SIS in Government	61
2. Ethical Issues of Using SIS in Government	63
2.1. Accuracy of Data	63
2.2. Accuracy of Algorithms	64
2.3. Technological Lock-in	65
2.4. Privacy and Security	65
3. DrukteRadar: Governmental Use of SIS	66
3.1. Description of Amsterdam's DrukteRadar	67
3.2. Description of SIS in the DrukteRadar Project	68
3.3. The Aims of the Organisation Using These Technologies	69
3.4. The Effectiveness of the SIS Technology during Use	70
3.5. Stakeholders Involved in the DrukteRadar Project	70
4. Ethical Implications	71
4.1. Access to SIS	72
4.2. Accuracy and Availability of Data	72
4.3. Accuracy of Algorithms	74
4.4. Ownership of Data	74
4.5. Technological Lock-in	75
4.6. Privacy and Security	75
5. Conclusion	77
5.1. Limitations	77
5.2. Contribution to Knowledge	78
5.3. Implications of this Report	78
5.4. Further Research	79
6. References	79

Executive Summary

Smart information systems (Big Data and artificial intelligence) are used by governments to improve mobility, reduce over-crowdedness in hotspots, and provide more effective management of crowds. I looked at how Amsterdam municipality is using smart information systems (SIS) in their DrukteRadar Project to identify, report, and tackle issues surrounding crowdedness levels in the city.

SIS are becoming popular amongst governmental officials to **automate activities** more effectively. SIS provide the opportunity to improve mobility, increase economic growth, reduce energy outputs, improve management decisions, respond to disasters quicker, and improve citizens' quality of life. They offer governments the possibility of **improving services, while reducing costs**. The use and implementation of SIS is becoming widespread and governments are observing the benefits posed by SIS, particularly in relation to **urban management**.

80% of Europe's population will live in cities by 2020 and governments face a huge strain on resources and infrastructure. The use of SIS is being pioneered to help governments meet these needs and to provide a sustainable future for urban citizens. Ethical issues in this context can include that data may not be **accurate**, faithful or representative of a city and its citizens, which may cause bias, prejudice and harm to a population, by leading to unfair service provision. ICT companies' involvement in governmental SIS projects may also lead to **technological lock-in** and dependency on corporations. Instantaneous and ubiquitous retrieval and analysis of data may infringe upon citizens' **privacy** and may lead to vulnerabilities of malicious hacking, stolen data and a city's **security**.

To uncover if these issues correlate with the experience of those working in the field, I interviewed the **Project Owner** of Amsterdam's **DrukteRadar project** (translated as crowdedness project). This project implements SIS to anticipate and prevent overcrowding in Amsterdam, and was created in response to growing pressures on the city's amenities. The DrukteRadar Project collates a wide array of datasets to predict crowd levels and potential problem hotspots, visualised through a digital dashboard. The project aims to improve **municipality management**, provide help to **tourists** planning their trips, and assisting **citizens'** navigation through the city.

Through my discussions with the **Project Owner** of the DrukteRadar, I uncovered two additional issues not found in the literature: **access to SIS** and **data ownership**. The DrukteRadar team is concerned about **access to SIS** to promote fairness, equality, and provision of services amongst citizens. It aims to make its dashboard user-friendly and available to as many people as possible to promote inclusion. **Data ownership** is a concern for the project – who owns the data and what can be done with it. The DrukteRadar Project ensures they have data sovereignty, so that they do not become **technologically locked-in** to relationships with private organisations.

The Project Owner was aware that **inaccurate of data** may lead to discriminatory recommendations and harmful consequences. The DrukteRadar Project tries to minimise their **algorithmic inaccuracy** through extensive monitoring; secure technical infrastructure; and stakeholder review sessions. Another interesting finding was identifying how projects ensure **privacy** protection of its citizens. The DrukteRadar ensures that data is not traceable to individuals and the use of datasets follow privacy-by-design principles. The project also has strong **security** protocols, cyber-security measures, anonymization techniques, and repeated vulnerability tests. Overall, my report was able to evaluate how ethical issues found within the SIS literature correlate to those identified, and tackled, in practice. as well as highlighting the two additional concerns not explicitly mentioned in the literature.

Government, Smart Information Systems, and Ethics

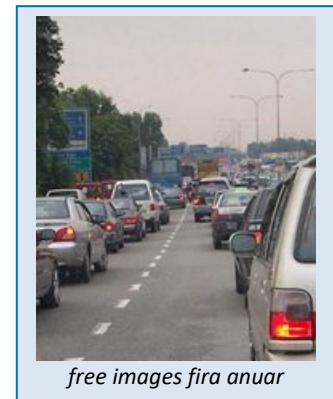
In 2050, 70% of the world's population will live in cities by 2050 accounting for 80% of the world's CO2 emissions (Nigon et al. 2016). 80% of Europe's population will live in cities by 2020 (Albino, Berardi, and Dangelico 2015).

Due to the large and growing populations, many cities currently face a huge strain on resources, infrastructure and transportation whilst simultaneously battling with pollution. The use of smart information systems (Artificial Intelligence and Big Data) are being pioneered to help governments meet these needs and to provide a sustainable future for their citizens.

This case study will evaluate a practical example of such efforts, namely the DrukteRadar Project in Amsterdam. One of the aims of the project is 24/7 digital congestion management.

Based on the literature and the DrukteRadar Project, this case study will analyse the ethical and social implications of using smart information systems (SIS) in the governmental domain, asking the primary research question: Which ethical issues arise in the use of SIS in governmental domains and how can they be addressed.

Section 1 will give an overview of the benefits of using SIS in government contexts and provide examples of how they are used in practice. Section 2 will analyse the current literature on ethical and social implications of using SIS in government. Section 3 comprises background research on the DrukteRadar Project in Amsterdam. Section 4 focuses on ethical and social issues in the DrukteRadar Project. Interview excerpts and results from talking to the Project Owner of the DrukteRadar are provided in both Sections 3 and 4.



1. The Use of SIS in Government

Smart information systems (SIS) offer the promise of improving services provided to citizens while reducing costs for city administrations (Zanella et al., p. 23). Big Data will underpin the future of urban data analytics, and will be an important component within governmental agendas (Bibri 2018, p. 193). The use and implementation of Artificial Intelligence (AI) and Big Data are starting to be widespread and governments are observing the benefits of SIS through improved infrastructure, mobility, and healthcare management.

According to some authors, SIS offers the potential to make governments more efficient, citizens happier, businesses more prosperous, and the environment more sustainable (Yin et al. 2015). SIS allow governments to: improve facilities, improve mobility, develop new services, increase economic growth, increase productivity, reduce energy outputs, improve air and water quality, improve management decisions, respond to disasters quicker, create new business opportunities, and improve citizens' quality of life (Kitchin 2014; Kitchin 2016a; Nam and Pardo 2011; Pan et al. 2016).

(SIS) offer the promise of improving services provided to citizens while reducing costs for city administrations.

SIS are being used in a wide number of different areas within the governmental domain, namely: healthcare, homes, governments, offices, transport, decision-making, security, e-service, and agriculture (Rjab and Mellouli 2018). Some examples are given below.

Yokohama, are implementing AI to aid them with their growing elderly population (Boenig-Liptsin 2017, p. 18)

Picture Freeimages, fabel nard



San Francisco police use the ShotSpotter AI tool, which uses neural networks to detect gunfire by listening for 'sound signatures' (Srivastava, Bisht, and Narayan 2017).

Picture Freeimages, José A. Warletta



50 AI cameras are being trained to prevent drunk passengers from boarding trains in Kyobashi (Osaka) (ibid.).

Picture Freeimages, Midori Sakurai



Drones are being used in fire control in Kansas, US by gathering data about a fire before firefighters are deployed (ibid.).

Picture Freeimages, Sias van Schalkwyk



AI has the potential to assess complex data streams, such as traffic congestion and mobility (Devi and Neetha 2017). The E-Taoyuan and U-Taoyuan projects in Taiwan are implementing e-governance strategies and options for citizens (Albino, Berardi, and Dangelico 2015). SIS may also be used to detect poverty and whether certain actions are improving wealth distribution levels (Glaeser et al. 2018).

There is an abundance of data being retrieved from cities in the hope of applying this information in effective and productive ways for its citizens. The main purpose of using and implementing SIS is to adequately accommodate citizens' needs (Chin, Callaghan, and Lam 2017, p. 2055). However, the different *categories* of stakeholders involved is quite diverse: private companies, philanthropy organisations, research agencies, universities, institutions, governmental bodies (regional, national, and international), city administrators, and NGOs. For the use and implementation of SIS, SIS specialist bodies are being created: regional bodies, national bodies, specialist units within existing bodies, international specialist institutions and lobby groups, as well as international standards bodies (Kitchin et al. 2017; Yin et al. 2015).

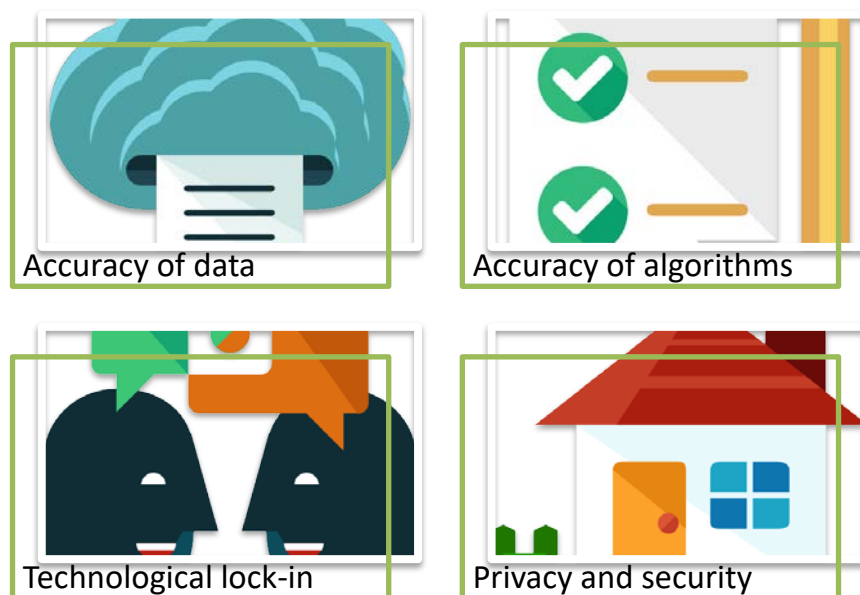
One of the key challenges facing governments is mobility planning and it is hoped that SIS will enable viable solutions in this area (Vázquez Salceda et al. 2014). Big Data can be used to change traffic lights based on the most conducive way for traffic to flow, which in turn is based on patterns

and real-time traffic flow. Big data can also be used to map and correlate the consequences of implementing particular changes in traffic management, i.e. ‘by closing a road or siting a new hospital on the network’ (Kitchin 2016c, p. 3). It is hoped that SIS will be able to provide effective and efficient methods to initiate appropriate changes to these structures. As European populations living in cities will increase to 80% by 2020, there is a growing concern about crowdedness levels within cities. One approach being implemented to combat this is Amsterdam’s DrukterRadar project, which is the focus of this case study. However, firstly, it is important to analyse ethical issues found in the literature relating to governmental SIS to be able to contrast this with issues found within the Dutch project.

2. Ethical Issues of Using SIS in Government

The extensive literature review undertaken for this case study used the following bibliographical databases: Google Scholar, ScienceDirect, Web of Science and Scopus. An array of keyword combinations was used to find articles about ethical issues arising from the use of Big Data and AI in governmental contexts. Because of the vagueness of the term ‘governmental’, several different keyword compositions were needed to allocate appropriate articles, such as city, municipality, government, state, national, and the public. As a result of the literature search, four key ethical issues emerged: accuracy of data; the accuracy of recommendations; power asymmetries; and privacy.

Figure 1 – Key Ethical Issues in the Literature– Using SIS in Government



2.1. Accuracy of Data

There is a shift from the old way of correlating and analysing datasets, which involved physically gathering data by conducting surveys, census, interview data and so forth. These required extensive labour-resources and the findings were highly irregular; monthly, bimonthly, or yearly. With many of the real-time, instantaneous ways of gathering and analysing data, one can instantly create reports and analytics. However, with the ubiquitous drive to find valuable information from Big Data, there is the possibility that important information is lost from traditional small datasets (Kitchin 2013, p. 265). Not only is there the possibility that one may lose important factors contained within small

datasets if only Big Data analytics are used, but one may also be limited by the ability to create integrated models that can effectively analyse this data (Batty et al. 2012).

The data derived and used to make decisions for cities are not value-neutral or impartial (Kitchin 2015a, p. 15). Data is not objective, it is always contextually loaded: established, derived, related and integrated within a wider information and logistical system. Therefore, data may not be accurate, faithful or representative of a city. There is the possibility that the data has errors within it, it may be inconsistent or unreliable (Kitchin, Lauriault, and McArdle 2015, p. 28). Analysing particular city indicators to find particular details may lead to overfitting and ‘generalize beyond the data an urban analyst is looking at in a particular context’ (Bibri 2018, p. 197). Therefore, it is important to identify potential misclassifications of data and applying data models to potentially incompatible urban data frameworks (Bibri 2018; Glaeser et al. 2018).

Data is not objective, it is always contextually loaded: established, derived, related and integrated.

2.2. Accuracy of Algorithms

The philosophy that underpins governmental SIS projects is often criticised as being limited in scope and ‘not provid[ing] a full and multidimensional picture of the city’ (Kitchin 2016b). Analysing Big Data may reduce cities to specific, definable and operable dimensions, conflating many important factors that define a city. This reductionist approach may fail to acknowledge the richness of how a city has functioned ‘socially, culturally, politically and economically’ (Kitchin 2013, p. 264). There is the belief that cities, guided by SIS, are ‘largely rational, mechanical, linear and hierarchical ... and can be steered and controlled’ (Kitchin 2015a, p. 9; see also Creemers, 2018). In SIS projects, cities may be treated as these knowable, predictable, and guidable entities, when in fact, they are a complex interweave of issues, problems, interests and uncertainties (Kitchin 2016a).

While AI is used to calculate and predict certain behaviours and patterns within the city, there are limitations on its effectiveness. Even though AI can help us with ‘highly routinized’ patterns, ‘there are limits on the extent to which we can explain them and reproduce them’ (Batty 2018). There is the possibility that SIS will cause bias, prejudice and harm to a population (Sholla, Naaz, and Chishti 2017). For example, predictive policing is criticised for reinforcing prejudices and racial profiling (van Zoonen 2016, p. 476). When human bias is put into AI algorithms, city services may not be provided equally or fairly (Capgemini Consulting 2017).

A potential issue along these lines was experienced in Boston, where a smart phone app was proposed to uncover potholes on public roads through automated recognition by the phone’s accelerometer¹⁴. “People in lower income groups in the US are less likely to have smartphones, and this is particularly true of older residents, where smartphone penetration can be as low as 16%. For cities like Boston, this means that smartphone data sets are missing inputs from significant parts of the population — often those who have the fewest resources” (Crawford, 2013). In the event, this was recognized before the app was used, and so the issue avoided. However, similar cases may have less foresight in this regard and recommendations based on such efforts would be biased.



Smartphone data sets are missing inputs from significant parts of the population — often those who have the fewest resources.

¹⁴ An instrument that measures the acceleration of a moving body.

For data analytics to have a prescriptive component, there need to be specific benchmarks established prior to data analysis and recommendations. ‘Benchmarking and dashboard initiatives thus inherently express a normative notion about what should be measured and how it should be measured’ (Kitchin, Lauriault, and McArdle 2015, p. 29). As a result, these benchmarks have the potential to guide discussions, set research agendas, influence governance, and ensure effective decision-making. Establishing unfair or inaccurate benchmarks may have a dramatic effect on issues being evaluated, citizen welfare, and the city as a whole.

Furthermore, there is the possibility that data retrieved from citizens will be used to ‘nudge’ them in certain directions and conduct activities they may not have performed otherwise (Cardullo and Kitchin 2017). Citizens may be manipulated in a socially-controlled manner, nudging individuals and groups in a particular direction (Kitchin 2018, p. 25). There is the possibility that SIS will be used to socially engineer a population, either to conform to particular practices and behaviours instituted by governmental bodies, which may also lead to power and control issues.

2.3. Technological Lock-in

There is a heavy financial burden to adopt SIS in the short-term, despite holding the potential to save more money in the long-term, so it is debatable if this is the best means of governmental expenditure (Glasmeier and Christopherson 2015, p. 7). Big Data storage facilities, research and innovation, data analysis and implementation, all incur high costs (Hashem et al. 2016, p. 749). Government use of SIS are not guaranteed to become successful and there is a great deal of uncertainty about return on investment. Cities implementing SIS are aiming to propel the development of their city, but this is not always possible; such as the Assen Smart City Project, which lost €50 million by installing over 200 sensors around the city (Cloin 2017). This ready-to-go ‘Sensor City’, it was hoped, would attract ICT investment. This did not happen. The municipality now has to find a private company to purchase the outdated sensors at a fraction of the investment (Naafs 2018). This money could have been much better spent elsewhere.

If corporations are heavily involved with any SIS government project, the city may become overly dependent on those corporations, putting public decision-making and governance in jeopardy (Kitchin 2015b, p. 2). Another concern about the adoption of SIS is that they will increase levels of privatisation of public goods (Kitchin 2016a, p. 23). SIS may drive the privatisation of state services and facilities. Public space, state services and facilities may become commodified, privatised, and used for advertising purposes (Hollands 2015, p. 68). As future cities will be run and controlled by electronic means, how a city functions and operates may be open to attack from third-parties (Batty et al. 2012). This may cause a wide range of problems for governments, particularly relating to the privacy and security of its citizens.

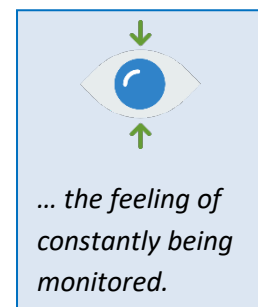
2.4. Privacy and Security

Individuals are being traced at multiple and varied routes along their journeys within cities and ‘are increasingly becoming open to geo-targeted profiling and social sorting’ (Kitchin 2016c, p. 8). One’s location may be used for stalking, burglary, surveillance, or marketing purposes (Elmaghraby and Losavio 2014; Li et al. 2016). One such example of this is how Renew installed sensors on 200 London bins in 2014, in order to track over four million individuals through their smartphone MAC addresses: ‘The company reported that they could measure the proximity, speed and manufacturer of a device and track the stores individuals visited, how long they stayed there, and how loyal customers are to particular shops’ (Kitchin 2016c, p. 7). While government officials state that they did not use this data for purposes other than to improve the functionality of the city, it does not mean that such means will not be used for surveillance in the future.

One’s location may be used for stalking, burglary, surveillance, or marketing purposes/

Another key concern relating to privacy protection and governmental implementation of SIS is ‘identity privacy’. Identity privacy is the protection of personal and confidential data about individuals’ identity (Kitchin 2016c, p. 5). For example, identifying who is using smart parking services or accessing smart buildings (Martínez-Ballesté, Pérez-Martínez, and Solanas 2013). Cities are anonymising and repurposing data in order to be able to use it. However, this data may be de-anonymised in the future. There are also a growing number of unmanned aerial vehicles (UAVs) using cameras, image repositories, and AI-technology to identify individuals; even if those individuals are not doing anything illegal or untoward. These technologies have the potential to harm identity privacy through SIS, such as AI-generated facial recognition.

Real-time analysis is fundamentally important for governmental SIS because it allows realistic planning of issues that require constant monitoring, updating and adjusting. However, having persistent, instantaneous and ubiquitous retrieval and analysis of data may have a seriously negative effect on citizens’ way of life, with the feeling of constantly being monitored. The adoption of SIS may lead to ‘dataveillance’¹⁵ and extensive geosurveillance, social and spatial sorting, and anticipatory governance’ (Kitchin 2015a, p. 9). In order to counter this effect, citizens should be informed about how their data is being handled, what it is being used for, how it will be stored, and who will have access to it (Galdon-Clavell 2013, p. 720).



There is the possibility that sensitive information may be retrieved, jeopardising the city’s functionality if this information is used nefariously. The greater digitalisation of the city infrastructure, the greater the vulnerability to malicious hacking, stolen data, or disruption of systems within the city (Kitchin, Lauriault, and McArdle 2015, p. 20). The costs of security may prevent cities from implementing SIS, causing a trade-off between costs and secure systems (Sen et al. 2013). There is a tension between cost-effective data retention, resulting in shorter storage times and diminished data usability, and incurring higher costs for improved data storage (Li, Cao, and Yao 2015). If there are inadequate security protections, citizens may reject SIS implementation (Zhang et al. 2017).

Having now discussed the ethical issues that the literature has identified with regards to the governmental use of SIS, it is clear that these cover a broad array of issues, most of which are not specific to governmental use. In order to better understand the way in which these issues arise practical contexts, the next section describes a case of a governmental SIS. The case was chosen because this project is using a large abundance of different datasets, obtaining public and private data to make predictions for the benefit of citizens and the departments within the municipality. The project is a unique way of integrating and using SIS in a governmental context, which could prove to be an innovative application that would be beneficial for all busy cities around the world. However, pioneering projects also come with their disadvantages, namely, that there are no similar projects to compare and contrast them with, and often ethical evaluations have not been carried out on them. Therefore, it is important that they are critically evaluated by third-party organisations (such as SHERPA) to determine their ethical viability and societal impact.

3. DrukteRadar: Governmental Use of SIS

The focus of this section will be on a governmental use of SIS in practice, namely, Amsterdam’s DrukteRadar Project, which loosely translates as ‘crowdedness project’. While the project is in its

¹⁵ The practice of monitoring digital data relating to personal details or online activities.

early stages of development, it can offer some insights about SIS projects being implemented in Europe in a governmental context. Interviews were conducted with the Project Owner of the DrukteRadar, a computer scientist working on it, and a further colleague working on the project. The computer scientist and the other colleague working on the project were not formally interviewed, thus not quoted in the case study. The interviews were analysed using a qualitative analysis software tool (NVIVO).

3.1. Description of Amsterdam's DrukteRadar

Amsterdam is the capital, and largest city, of the Netherlands, with the municipality comprising of over 200 km². The 850,000 Amsterdammers are proud of their city and the municipality is always making improvements for the 180 different nationalities that inhabit it. Along with a highly condensed population, the city receives a staggering 18 million visitors a year and is the 8th most visited city in Europe. This number is set to jump to 25 million by 2025 (Hein 2016). Tourism accounts for over €75 billion in the Netherlands and consists of 3.9% of GDP, employing 641,000 people (Pieters 2018). The municipality realises the benefits tourism brings to the city and its dependence on ensuring that all significant sites are well-preserved, amenable, and accessible to visitors and locals alike. Tourism is very important for Amsterdam, but it comes with the cost of overcrowding. In recent years, Amsterdam municipality has attempted to take a proactive approach, initiating a number of innovative approaches, through their Chief Technology Office (CTO).



Amsterdam, photo: Peter Hellbrand, free images

One of the goals of the CTO is to create a roadmap to ensure the city is futureproofed. Its aims are to enable the city and its authorities to connect, accelerate and strengthen new projects and to create solutions to problems within the city. The CTO and the municipality have been involved in a number of projects in recent years such as:

- sharing traffic data with a technology company in order to help them tackle traffic congestion in the city;
- using data to identify depression hotspots to provide better care and services to those areas;
- “Beautiful Noise”, which assesses social media comments from museum queues to improve services;
- “Rain Sense”, which identifies places with bad rainfall to prevent flooding;
- smart street lighting; and
- pay-by-phone parking apps (Fitzgerald 2016).

The CTO is responsible for some of the most innovative approaches being implemented within the municipality, such as the DrukteRadar Project, the planning for which started in early 2017. The aim of the DrukteRadar Project is to use data analytics to anticipate and prevent

overcrowding in Amsterdam. The output of the project was supposed to be launched in the summer of 2018, but it was postponed until the second quarter of 2019 to ensure functionality and that it was fit-for-purpose. The interviewee for this case study is the Project Owner of the DrukteRadar. He is the person who has to make strategic decisions about the project's direction. He said that the project was funded for the next four years and had the full endorsement of the municipality. It is an innovative platform that is set to greatly benefit the city of Amsterdam.

3.2. Description of SIS in the DrukteRadar Project

The aim of the DrukteRadar Project, as noted earlier, is to use data science to anticipate and prevent overcrowding in Amsterdam. The project uses technological tools to create data about crowd levels in the city for effective use by locals, tourists, and city managers.¹⁶ It was created by the CTO and City in Balance¹⁷ group in response to growing pressures on Amsterdam's amenities, navigation, and tourist and citizen experience. The aim was to create a dashboard so that both the municipality and Amsterdammers could identify when areas of the city are crowded.

The project aims to identify potential crowd numbers from hotel stays, events, and crowd-size projections. This involves retrieving very large amounts of data from inside and outside of the municipality, while effectively analysing and visualising those data. The project first identified that in order to have a fully functional and successful crowd prediction model, they needed to collect and analyse large datasets. The data retrieved focuses on the number of people in particular areas, length of time they stay there, and problem areas. The CTO wants a wide array of Big Data from:

- i. Public transport: GVB, Connexxion, NS and Translink.
- ii. Private transport: TomTom, HERE, tech companies, TCA, the Municipality itself.
- iii. Pressure on locations: Google.
- iv. Telephone: Vodafone, T-Mobile and KPN.
- v. Hotel occupation: Booking.com, Airbnb.
- vi. Economic activity: Mastercard, ABN AMRO, ING, Rabobank.
- vii. Tourism & recreation: Tours & Tickets, Booking, AirBnB, Schiphol.
- viii. Social media: Facebook and Twitter.

All of the data retrieved from these different sources is stored on the municipality's data storage facility, DataPunt. This is a low-cost open-source storage space and the municipality places a great deal of emphasis on ensuring its security. DataPunt was created in early 2016 and is the data store function of Amsterdam Municipality. It has a number of modules that retrieve, link, and receive data as well as making this data accessible to other ICT systems. There is a need to develop the data landscape of the municipality and to effectively use and integrate data into helpful, manageable ICT processes (Moerman 2017, p. 7). Some of the data types are: 'Information about public space, buildings and lots, traffic, care, environment, quality of life, permits, subsidies and numerous other data' (Municipality of Amsterdam 2018). DataPunt is the municipality's storage facility and functions as the central data portal between the municipality and its partners. The large

¹⁶ The DrukteRadar operates through a number of docker containers, which are run on their server. There is a mixture of front-end, back-end, and databases connected through this network to run the dashboard. For the front-end, there is standard HTML, CSS and JavaScript, and Application Programming Interfaces (APIs) running in separate containers. The database is in a separate container and the importer transforms the data into the right format. They use weak patterns as complex machine-learning methods would over-fit the data.

¹⁷ It experimented with ways to find a better distribution of tourists in the city (City of Amsterdam 2019).

datasets stored in DataPunt are ready to be reused in Amsterdam projects, such as the Drukteradar.¹⁸

The project's dashboard is an interactive map of the city, with specific 'hotspots areas' map and a 'district level' map of the city. The hotspot map identifies how crowded specific locations within the city are. It is meant to inform Amsterdammers, tourists, and also those working in the municipality about particular locations in the city. There are also layers for automobile traffic, bicycle traffic, and pedestrian traffic in the city.

The district level dashboard identifies how crowded entire districts are and is designed for the municipality, rather than locals or tourists. The hotspot and district maps distinguish the crowdedness by colour coding: the lowest levels are green, with mid-levels shades of orange, and problematic areas are red. However, the way of measuring district and hotspots is different. The district level is measured on an objective person-per-square-meter metric, while the hotspot level is measured on a historical relative account of those areas (however, this may change to the more objective approach in the future).



3.3. The Aims of the Organisation Using These Technologies

There is a pressure on the city of Amsterdam to accommodate increasing numbers of people. Everyone wants to visit the same landmarks, which are centrally located or are within certain areas of the city.¹⁹ There is a concern about how the municipality will cope with the pressure on amenities in the city. As a result of these issues, there were a number of different approaches suggested in order to ensure that residents and visitors can enjoy the beautiful city with comfort and ease. One of the main issues raised was the need to identify problem areas, times of peak busyness, and ways to ameliorate these issues. In conjunction with different organisations and departments within the municipality, it was proposed that crowd management could be tackled by the program City in Balance, which created the Drukteradar Project.

The Drukteradar Project will collate a wide array of datasets to predict crowd levels, movement, and potential problem hotspots. The data will be used for better municipality management, for greater visibility for tourists planning their trips, and for citizens to navigate through crowds during their daily activities. One of the main benefits of this project is anticipated to be that the Council can implement better management decisions and strategies, as a result of increased knowledge of crowd levels. Different departments will need data on crowd levels for different reasons and the Project Owner's responsibility is to determine what they need from the data. So, for instance, the Waste Department asks the Project Owner to identify crowd levels so that they can ensure the city remains clean; the Transportation Department needs data to alleviate traffic congestion, and the Police Department needs data to identify potential problematic areas.

¹⁸ The data required by Drukteradar is sent from DataPunt, and is processed in the back-end docker container. The analyser container uses machine-learning and works with the database container, to find weak patterns emerging within the datasets. The developers have created an Application Programming Interface (API) that is used by the visualisation docker container to illustrate the crowdedness levels on a dashboard.

¹⁹ Tourists mainly congregate in the following areas: The Old Centre; the Museum District & Vondelpark; Oud-West; the Canal Belt and Jordaan. While other areas in Amsterdam are also witnessing increased volumes of tourists in recent years: De Pijp; Plantage; North Amsterdam; the Docklands; and Amsterdam Zuid.

3.4. The Effectiveness of the SIS Technology during Use

The Project outlines six specific steps to ensure the effectiveness of the DrukteRadar project:

Steps	Description	Details
1	Acquiring data	Individuals tasked with retrieving data within the city and externally.
2	Estimating and planning potential	Prioritisation of data retrieval is agreed upon, depending on the high level of impact and necessity.
3	Make good agreements	Identifying who manages the data and how it is used.
4	Database storage and API creation	Data is stored at DataPunt, which is under supervision of Amsterdam municipality.
5	Data processing and front-end development	Data is evaluated to determine specific issues and is made available to front-end developers for visualisation purposes.
6	Testing and development	The software is tested to determine if it is fit-for-purpose. End-users are consulted to identify issues with the tool.

The CTO will establish a number of different Key Performance Indicators (KPIs) and metrics to determine the success and worthwhileness of the project. While the project is still in its early stages, they want to identify a number of different metrics, such as:

- how many stakeholders will the project help to resolve issues;
- will the project help optimise garbage collection routes, also leading to a reduction of Co2 emissions and lower fuel costs;
- how many people use the website or the project and how do they use it; media coverage received; positive or negative feedback; and reductions in busy hotspots.

3.5. Stakeholders Involved in the DrukteRadar Project

The DrukteRadar aims to incorporate a wide range of stakeholders in its approach, and suggestions for further stakeholders are considered necessary to improve the project. The end-users are incorporated into the stakeholder group and are involved throughout the design and implementation of the project. The DrukteRadar Project Owner receives regular feedback from users and test panels, which are incorporated into dashboard developments.

The project team works in an Agile format, according to SCRUM principles,²⁰ and the Project Owner is responsible for the overall project. His main responsibility is transforming stakeholder input and feedback into concrete tasks for the development team to implement. The project also has an advisory group, consisting of scientific experts, where they provide advice on new priorities every six months. There is also a tactical management session every three months to identify potential issues. The stakeholder group consists of members from the following groups: V&OR; OOV; Smart Mobility; EZ; CTO; R&D; Parkeren; City Works; Clean Stadsdeel Centrum; Schoon; Afval; and OIS. This stakeholder group assists the project in developing the agenda and ensuring agreed standards are met.

End-users are involved throughout the design and implementation of the project.

²⁰ The SCRUM principles are: focus, openness, respect, courage and commitment ("Scrum Values & Agile Methodologies for Project Management," 2018).

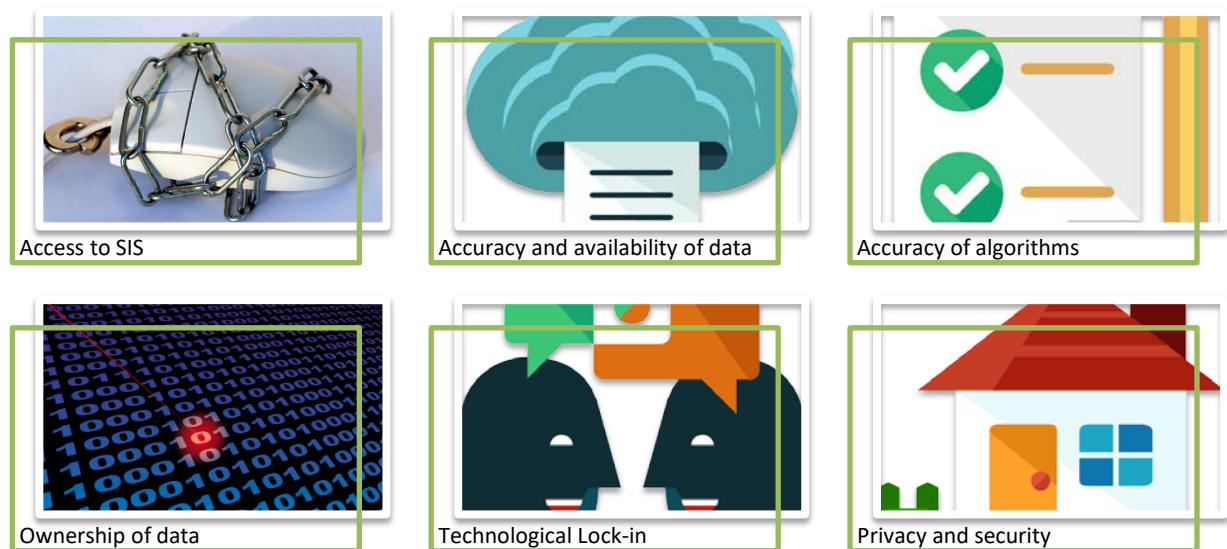
In order for the project to work successfully it requires internal and external data. The municipality wants to pay as little as possible for data. Currently, data providers only have data that is a week old, or even a month old, which is too old for the project's requirements. External data retrievers should therefore coordinate partnerships on behalf of the city of Amsterdam to obtain newer data. There needs to be a bridge between data providers and the municipal government. There is a legal memorandum of understanding (MoU) between the municipality and data providers to ensure agreement about their partnership. The municipality aims to incorporate prevalent public figures in the discussion of crowd management to retrieve insights into the development of the project. The Project Owner said that it is a hot topic in the media and the public is aware of the need for such intervention in the city. The project is considering the integration of a feedback option for citizens to provide recommendations. They want to make clear that there will be many iterations throughout the project's development.

The project will also contain a feedback option for citizens to provide recommendations.

4. Ethical Implications

After careful analysis of the DrukteRadar documentation, conversations with the team, and the interview with the Project Owner, a number of pertinent ethical issues were identified that may result from the project's implementation and use. The six ethical issues identified were: access to SIS; accuracy and availability of data; the accuracy of algorithms; ownership of data; technological lock-in; and privacy and security.

Figure 2 – Key Ethical Issues DrukteRadar project (some images from freeimages.com)



These topics were discussed during interviews and largely coincide with the ethical issues that are found within the literature on the topic of SIS implementation in a governmental context. Two ethical issues that did not specifically arise in the literature concerning the governmental use of SIS, but did arise in the interview, were access to SIS and ownership of data. Overall, there were a lot of similarities between what the project views as ethical concerns that need to be incorporated and what has been identified as concerns in the literature.

4.1. Access to SIS

The Amsterdam municipality is aware that most people are not technologically savvy, so it had to adopt a more bottom-up approach trying to make their actions as transparent as possible to citizens (Fitzgerald 2016; Grashoff 2017b, p. 3). One goal of the Drukteradar Project was to ensure that it was user-friendly and to make it available to as many people as possible. The effectiveness of the Drukteradar Project relies heavily on whether or not it is used, which relies on how it is disseminated. The Drukteradar team have identified that social media and Google were obvious dissemination channels, but *how* exactly this data would be distributed was a little unclear. The Project Owner noted that they were going to do two things to ensure availability and access to the Drukteradar: use the project for citizens and the public, but also provide it to other departments within the municipality to use.

He also mentioned that the project will disseminate its services through the dashboard, which was explained in section 3.2. of this case study. This visualisation will clearly show citizens where it is busy and what levels of crowdedness they can expect at a particular time. In order to ensure that citizens are made aware and have access to the dashboard, the municipality is going to begin a social media advertising campaign in 2019, through the city of Amsterdam website, and possibly through newspapers and other outlets. However, at the moment, this is not a top priority as they are more focused on having the project successfully deployed. Most of the data and documents are available on the municipality's open data platform, and for the success of the project, it is important that it has accurate and available data for its recommendations.

4.2. Accuracy and Availability of Data

One of the chief problems with implementing SIS is the lack of available data repositories. In itself, it is not an ethical issue, but as a result of poor-quality data repositories and data availability, algorithmic predictions may lead to discriminatory recommendations, inaccurate predictions, and harmful consequences. Data accuracy and availability is therefore an important concern for Amsterdam Municipality.²¹

Accuracy and availability of data issues are prevalent in the integration and use of emerging technologies, and one of the limitations for their effectiveness is the lack of available data to train their models. For example, the Drukteradar project requires more real-time data to improve their models. Data is only compiled from a few months previously, so the project is unable to give a cohesive evaluation and comparison of the levels of crowdedness of the previous year. The project needs to have larger, longer, and more detailed datasets so that they can produce more effective models. Otherwise, if they apply their current



²¹ Amsterdam's Chief Technology Officer mentioned that they found it difficult to calculate how many bridges they have in the municipality (Baron 2016). When Ger Baron took on the role of Chief Technology Officer he grew their inventory to 12,000 datasets, which allowed them to get a wider picture of problems facing citizens (Fitzgerald 2016). He noted that they also use analytics frameworks to assess small data so that they do not miss crucial data in these sets (Baron 2016). For example, the AMS Institute used Wi-Fi hotspots, cameras, GPS tracking and social media posts to determine crowd sizes, movement of crowds, and congestion areas during the 2015 SAIL Amsterdam Festival (Fitzgerald 2016). During this event, Baron noted that there was something delaying people at a point on the map and researchers made guesses about what this could be. In reality, there was a trash-can in that location, which was not on their map, and people were slowing down to throw rubbish into it (Fitzgerald 2016).

datasets to these models, they would be over-fitted²², which would be problematic for accuracy and effectiveness.

So far, the project has incorporated data from various sources in the municipality. Internal sources are a wide range of different city departments and groups, whereas external data is retrieved from different partner organisations of the municipality. It is often difficult to obtain the most effective and useful data for the project and as a result of the General Data Protection Regulation (GDPR) and other legislation, many departments are apprehensive about providing data to the project. In addition, the Project Owner highlights that sometimes it is difficult to get data from different departments because they want to see a benefit for providing this data. Even within the municipality, there needs to be a mutual benefit for data provision. The DrukteRadar team needs to identify how departments can benefit from the use of this tool if they provide their data repositories.

The Project Owner acknowledges that internal data has its limitations. He stated that when analysing the busyness of the city, less populated and more secluded areas have little data on how busy they are. Private organisations, such as telecom providers or Google Maps, have a greater availability of datasets covering wider ranges of the city. Another limitation with acquiring internal datasets is that it requires a great deal of time. He pointed out that it is a challenge to acquire these datasets because there needs to be a mutually beneficial relationship to acquire them.

‘So, if you can say that, “Give us the data, and we’ll make sure that you can run your external operations more efficiently”, then that helps. That’s the kind of win-win situation we want to create’ (Interviewee 1).

*Give us the data,
and we’ll make
sure that you can
run your external
operations more
efficiently*

In relation to external data, the project has ‘data hunters’ that deal with semi-public or private organisations to obtain appropriate data for their algorithms. The data hunter tries to negotiate partnerships with private companies to establish a mutually beneficial relationship. The private organisations benefit from having a big client like the Amsterdam municipality, and the project benefits from the provision of data. The Project Owner says that

‘they can fine-tune their business case, and together we can develop a project that’s also interesting for other similar cities and based on that partnership, we get the data for free, and they can use their insights they get from us for other cities’ (Interviewee 1).

The DrukteRadar Project aims to minimise the number of errors occurring, but it is important to have preventative and ameliorative steps in place for when they happen. If there are errors or discrepancies within city data, Amsterdam has a number of contingency plans in place: it has extensive monitoring facilities, and a secure technical infrastructure (Gemeente Amsterdam 2018b). A range of questions have to be asked in terms of the data derived, such as:

- is the data suitable,
- where does it come from,
- who has access to it,
- is it current,
- and how is it managed (Moerman 2017, p. 5)

²² Overfitting a model is when there are more parameters inputted than are justified by the data provided. It is attempting to extract richer, more nuanced information from limited datasets.

Furthermore, to ensure that their data is accurate and effective, the DrukteRadar Project provide the general public with the option to contact them if they identify any problems with the product's recommendations (Gemeente Amsterdam 2018a). It is important to establish accurate and effective data so that the municipality can make accurate and appropriate recommendations and predictions, thus minimising any harmful effects as a result of improper measures and policy.

4.3. Accuracy of Algorithms

The DrukteRadar Project, initially implemented relative data measurements for the hotspot levels in cities and objective data measurements for the district-level dashboard. However, there is a concern about using different methodologies to depict the crowdedness level in the city, with the district level applying persons-per-square-meter, whereas the hotspot level applies the historical relative account of crowdedness.

The hotspots are compared against historical data, and against what a 'typical Thursday' looks like; while seasons or other variables are not accounted for, yet. The amount of historical data only extends back a few months, making it impossible to give an annual forecast or projection. There are options to increase and decrease the approximate levels depending on seasons, but the methods used might be inaccurate. The hotspot measurement identifies a particular location. For example, the level of busyness of Dam Square at 13:00 on a particular Saturday is assessed against what the standard level of busyness for Dam Square on a Saturday at 13:00 (relative data), rather than how busy Dam Square is compared to other locations in the city (objective data). This is to cater to locals so that they can identify areas that may be problematic for their commutes or activities, while also acknowledging that there are certain areas that will always be quite busy, such as Dam Square.

However, one would need some previous knowledge and understanding of areas within Amsterdam to unpack this information, making it difficult to cater to both tourists and locals alike. The tourist may not understand the relative index being used in the project; for example, knowing that Dam Square at a medium level of business is still very busy. This may make it difficult and confusing for the non-local user. If the project uses two different maps, one for the local and another for the tourist user, it may also be problematic because the local may not be able to interpret what a standard level of busyness is for an area. For example, what if they are a local but have never been to that particular landmark in the city so are unaware how busy it is regularly, or perhaps they are local, but new to the city.

The Project Owner mentioned that an important issue for the project was to identify who the end-user will be and then design the platform based on this understanding. The needs of a citizen of Amsterdam would be different from a tourist, which would be different from departments within the municipality using it. Once the team finalise who the end-users will be, they will be able to create different landing-pages, structuring the data visualisation according to their needs. He noted that they recently veered towards using more objective data, rather than relative data, for identifying the hotspot busyness level of the city.

4.4. Ownership of Data

One of the explicit goals of the DrukteRadar Project is to ensure data sovereignty. While Ger Baron agrees with the need to incorporate SIS in Amsterdam, he claims that tech companies do not always understand cities and how they work, emphasising that what works in theory does not always work in practice (Baron 2016). Models and technological propositions may confine and reduce the complexity of a city such as Amsterdam. Baron states that they would have left a great deal of technological innovation to the companies in the past, but he has been looking closely for governmental involvement in recent years (Baron 2018). He wants to take a stronger role in SIS

development, as he believes that they can 'deal with this much more effectively and efficiently' (Baron 2018).

When the municipality works with private organisations to evaluate data, and use it for the DrukteRadar's functionality, sometimes the issue of data ownership is raised. The Project Owner indicated that the ownership of data depended on where the data was collected from. If the municipality creates the data, then it is the owner of this data; whereas, if the partner organisation creates the data, then they claim ownership of it. If the data is collected in a public space, then the city of Amsterdam tries to ensure that they obtain ownership of that data. This is achieved through contracts and partnerships with private organisations.

The relationship between the municipality and internal and external data providers is a data partnership. The Project Owner stated that the organisations' role is a data provider and they have no control over the running of the project. Both internal and external partners do not have any involvement or say in how the project is structured, organised, or how they create their models. They have a vested interest in the success of the project, either for personal use (internal partners) or having Amsterdam municipality as a customer (external partners). The DrukteRadar Project aim to ensure a mutually beneficial relationship is achieved between public and private entities with a high degree of data sovereignty.

4.5. Technological Lock-in

There will always be tensions between public and private interests in the use and implementation of SIS in governmental applications. Ger Baron stated that the city of Amsterdam pushed back on companies from installing transmitters and sensors on street lamps around the city because it was not in the public's interests (Baron 2016). Amsterdam rejected the idea to install smart lighting because of the extremely high costs of investment (Fitzgerald 2016). The municipality tries to succeed with an independent approach from third-party companies, but often this is not possible.

The DrukteRadar project has already come up against problems attempting to establish a data-sharing partnership with a bank, but the bank's lawyers opposed such a relationship. While some telecommunications companies will not even discuss this topic with the municipality of Amsterdam. The CTO has realised that obtaining data from third-party organisations is not easy and often requires considerable costs. Often, these third-party organisations want a collaborative arrangement in order to benefit both parties.

The municipality is in the process of setting up arrangements with NS and Schiphol airport to create data sharing partnerships. There is the hope that these agreements will be mutually beneficial, rather than Amsterdam purchasing or becoming a customer of these organisations, rather than Amsterdam municipality necessarily being dependent or locked-in to relationships with these organisations. The Project Owner mentioned that one way of creating this partnership is data-sharing.



4.6. Privacy and Security

Because data is being retrieved about citizens, their location, their time spent there, and because these data may be linked to what they are doing there, there is a concern over privacy for the DrukteRadar Project and how to ensure that it is protected. The project has a mixture of objective data, but only uses aggregated data from a minimum of 15 people so that it is impossible to identify individuals from the group. In instances where the number of people in an area is below 15, the

system would produce a result of zero, in order to ensure that individuals are not identifiable to ensure privacy. Fundamentally, the project does not want

‘any personal data of any sort. And we actually want as little data as possible; just the necessary data that we can use to run our models, and make it as efficient as possible’ (Interviewee 1).

There are a number of different data sources being retrieved, ranging from low to medium privacy risk. For example, weather data has no privacy concerns, whereas, park and ride data (which shares how many spots are being used) and NDW traffic data (such as speeds on the road and average speeds) have a low privacy risk, because of the lack of personally-identifiable information. The data retrieved from bike rental has no personalized data, just the quantity of bikes; and public transportation data is protected by having specific cut-off values as described earlier.

The city aims to protect citizens’ privacy as much as possible and claims to ensure that the open data that is available on their website is not traceable back to any individual person (City of Amsterdam 2018). They do this by ensuring that no individual’s data is input in the first place and any datasets that are used follow their privacy-by-design principles. The Municipality explicitly state that an individual’s data will never be given to commercial institutions or private individuals unless written permission is granted. In addition, one can request that one’s data is not shared with non-mandatory administrative authorities. The DrukterRadar team ensure that

‘every data source we use has the privacy-by-design incorporated in the source. So that means that privacy is designed within the data collection mechanism’ (Interviewee 1).

Partners providing data must follow strict adherence to the organisation’s privacy-by-design principles. This is carried out at the start of any collaboration with different internal or external partners. Internally, it is achieved by the privacy officers within the city itself,

‘we actually want as little data as possible; just the necessary data that we can use to run our models efficiently’

‘who advise on these projects, and they always advise to collect no personal data, or at least as little as possible’ (Interviewee 1).

The privacy officers ensure that no personal information is passed on in the datasets and that all the privacy concerns are adhered to. The project only wants to use and have access to non-private information. The Project Owner mentioned that sometimes this can take a lot of time with back-and-forth communications between different departments and privacy officers, but that they wanted to ensure they meet current privacy protection standards.

‘Normally all the data that’s open, or that’s not privacy related, we can share’ (Interviewee 1).

He elaborates that the open data does not contain any private or personal information of any of the citizens of Amsterdam, as they do not store or retrieve any personal data or personally identifiable information. They place a strong focus on ensuring the privacy of its citizens is protected. In relation to external datasets, the Project Owner pointed out that the level of aggregations of these datasets makes it impossible to extract personally identifiable information. However, the department still ensures that external partners also abide by the seven privacy-by-design

principles.²³ In addition to implementing privacy protocols, the project also protects privacy by ensuring that all data is safely secured on the municipality's data storage system.

The DrukteRadar uses data from DataPunt, which is a heavily secured cloud system, used to store and collect data. DataPunt is the Amsterdam data node facility that makes information about the city open and available (Grashoff 2017b). They emphasise that distribution of data is only provided to those that need it and respecting legal requirements (i.e. in accordance with national, EU, and municipal legal regulations). Amsterdam Municipality protects this data from being hacked and compromised. DataPunt minimises privacy risks by reducing the amount of personal data permanently stored, strengthened cyber-security measures, anonymization techniques, and repeated vulnerability tests (Grashoff 2017b). The DrukteRadar follows the principles outlined in DataPunt to ensure security levels are met. The Project Owner claims that it is very secure and reliable.

5. Conclusion

SIS may be used by governments in a wide diversity of applications, which can result in a wide range of social and ethical issues. This case study evaluated ethical and social issues found in the literature, how SIS is being used, and what actions are being taken to counter harmful impacts on society. The case study evaluated a specific application of governmental SIS, the DrukteRadar Project, to provide context for how municipalities are dealing with ethical issues. Focusing on the use of SIS in Amsterdam, provided key insights into ethical issues and how they contrast with those found in the literature.

The interview with the Project Owner provided information about the real-life application of governmental SIS while addressing a number of ethical issues as a result: access to SIS; accuracy and availability of data; accuracy of algorithms; ownership of data; technological lock-in; and privacy and security, which are being addressed by the DrukteRadar team.

The DrukteRadar team are ensuring that stakeholders are made aware of the dashboard developed for the project through a public awareness campaign on social media, newspapers, and their website. The DrukteRadar team realise that accuracy and availability of data underpin the success of their project, so they have been establishing partnerships with internal and external data providers. The municipality also wants to maintain its data sovereignty, so the project tries to concentrate on using internal data to guarantee data ownership and avoid technological lock-in. The project also ensures that datasets follow privacy-by-design principles and are GDPR compliant.

5.1. Limitations

A notable limitation of this case study is that it is analysing SIS that have not been fully implemented and disseminated to its target audiences. When I first contacted the organisation, the project was supposed to be launched by October 2018, but this date was pushed back until Spring 2019 because the team wanted to refine it before launch. While many of the issues raised in this case study are pertinent, there may be additional issues that are only visible once it is implemented and used in practice. This could have been valuable exploratory terrain for the case study.

One of the main limitations of this case study is that it was based on only three interviews, only one of which was analysed in a structured manner. While the primary interviewee was

²³ The seven principles are: proactive not reactive; privacy as the default setting; privacy embedded into design; full functionality: positive-sum, not zero sum; end-to-end security: full lifecycle protection; visibility and transparency; and respect for user privacy ("The Seven Foundational Principles," 2018).

knowledgeable about SIS and their societal and ethical impacts, the case study would have been strengthened by additional interviews. Furthermore, as the case study only examined one example of SIS in Amsterdam, it does not allow for generalisations about their use of SIS, or broader conclusions about municipalities' use of SIS, generally. The project also focused on a specific application of SIS (i.e. for crowdedness detection and prevention), which would make it impossible to difficult to make broader deductions about the use of SIS by governments.

5.2. Contribution to Knowledge

This case study offers the discipline a fresh look at the ethical concerns associated with using SIS in a governmental setting. While some of the topics and issues discussed in this case study have been evaluated elsewhere, they have rarely been applied to specific projects in this way. Therefore, the case study has specific implications for SIS ethical theory and analysis. Furthermore, there has been very little written about Amsterdam's ICT projects, besides self-published articles on their websites. This case study offers the municipality an objective evaluation of one of their latest projects, prior to its full-scale implementation, and ethical issues that may arise in the project's development.

The analysis of the DrukteRadar Project contributes an empirical evaluation of SIS being used in practice, uncovering two specific issues that were not found in the literature: access to SIS and data ownership. It was shown that a municipality can increase access to SIS, promoting fairness, equality, and provision of services amongst citizens. The DrukteRadar project achieves this by ensuring that its dashboard is user-friendly and available to as many people as possible.

While there are general policy guidelines and frameworks for the ethical use of SIS, there are few recommendations specific applications of SIS, particularly around data ownership and relationships between public authorities and private companies working on SIS. The case study offers insights into how municipalities can tackle the issue of data ownership, namely, if the data is collected from a public space, then the city should claim ownership, rather than private companies.

5.3. Implications of this Report

This report has policy implications for the use of SIS within the governmental domain, particularly municipalities. When cities integrate SIS, there should be ethical considerations about how they will affect citizens, the city's relationships with private companies, and their impact on society.

One way to do this is by identifying who the end-user is during the design phase of SIS. Cities need to acknowledge that a lot of people are not technologically-savvy. The effectiveness of public SIS depends on whether or not it is usable and available to most people. Policymakers should have clear dissemination plans to reach their end-user, in this case, the citizens of Amsterdam. Municipalities may use this case study to understand important concerns related to the implementation of SIS. This report showed that there needs to be a win-win scenario in data partnerships, whether they are public or private.

However, what became evident in this case study is that private companies may not always understand how cities work, so city officials need to be careful when collaborating with them on SIS projects. Departments within the municipality may deal with tasks more efficiently and effectively than private companies. Investments into training internal staff, instead of outsourcing projects to costly ICT companies, is something that should be considered. This case study also demonstrated how ensuring data sovereignty could help avoid becoming technologically locked-in and dependant on private organisations.

This report provides policymakers with fresh insights into how they can reduce discriminatory recommendations and harmful consequences resulting from SIS – through extensive

monitoring, secure technical infrastructure, and stakeholder review sessions. Technical insights were provided to show how cities can ensure citizens' privacy is protected: data is not traceable to individuals (aggregated data from a minimum of 15 people), internal and external datasets follow privacy-by-design principles, and try to obtain as little personal data as possible. Finally, this report provides ways municipalities can ensure data security: use a heavily secured cloud system, anonymization techniques and repeated vulnerability tests.

5.4. Further Research

The literature review aimed to provide an overview of the main ethical issues being discussed in governmental use and implementation of SIS. Additional research may need to be completed on ethical issues that arise in the future relating to governmental applications of SIS. There is a need for further empirical investigations into the use of SIS by governments, through discussions about how cities are using SIS, as well as how different international institutions, or supra-international bodies, are using SIS. Furthermore, additional case studies may allow for cross-case analysis with other empirical research on SIS use. Overall, the hope is that this report encourages more academic evaluations into the ethical use and implementation of governmental SIS.

6. References

- Albino, Vito, Umberto Berardi, and Rosa Maria Dangelico, "Smart Cities: Definitions, Dimensions, Performance, and Initiatives", *Journal of Urban Technology*, Vol. 22, Issue 1, 2015, pp. 3-21.
- Amsterdam Smart City, "Perspectives on the Future of Mobility in Amsterdam", *Smart Mobility in Amsterdam*, 26th March 2018.
- Baron, Ger, [Interview], in Fitzgerald, Michael, "Data-Driven City Management: A Close Look at Amsterdam's Smart City Initiative", *Sloan Review*, May 19th, 2016, <https://sloanreview.mit.edu/case-study/data-driven-city-management/>
- Baron, Ger, [interview] in Daalder, Leonieke, "Ger Baron (CTO of the Municipality of Amsterdam): 'How do we go from Government to GovTech?'"', Marketing Facts, 6th March 2018: <https://www.marketingfacts.nl/berichten/ger-baron-cto-gemeente-amsterdam-overheid-govtech>
- Batty, Michael, "Artificial Intelligence and Smart Cities", *Environment and Planning B: Urban Analytics and City Science*, Vol. 45, Issue 1, 2018, pp. 3-6.
- Batty, Michael, Kay W. Axhausen, Fosca Giannotti, Alexei Pozdnoukhov, Armando Bazzani, Monica Wachowicz, Georgios Ouzounis, and Yuval Portugali, "Smart Cities of the Future", *The European Physical Journal Special Topics*, Vol. 214, Issue 1, 2012, pp. 481-518.
- Bibri, Simon Elias, "Data Science for Urban Sustainability: Data Mining and Data-Analytic Thinking in the Next Wave of City Analytics", *Smart Sustainable Cities of the Future*, Springer, Cham, 2018, pp. 189-246.
- Boenig-Liptsin, Margarita, "AI and Robotics for the City: Imagining and Transforming Social Infrastructure in San Francisco, Yokohama, and Lviv", *Artificial Intelligence and Robotics in the City*, Issue 17, 2017, pp. 16-21.
- Capgemini Consulting, "Unleashing the Potential of Artificial Intelligence in the Public Sector", Capgemini website, 2017, retrieved 27th July 2018:

- <https://www.capgemini.com/consulting/wp-content/uploads/sites/30/2017/10/ai-in-public-sector.pdf>
- Cardullo, Paulo, and Rob Kitchin, "Being a 'Citizen' in the Smart City: Up and Down the Scaffold of Smart Citizen Participation", *The Programmable City Working Paper 30*, SocArXiv Website, 15th May 2017.
- Chin, Jeannette, Vic Callaghan, and Ivan Lam, "Understanding and Personalising Smart City Services Using Machine Learning, the Internet-of-Things and Big Data", *IEEE 26th International Symposium on Industrial Electronics*, 2017, pp. 2050-2055.
- City of Amsterdam, "City Data", *Gemeente Amsterdam* [website], retrieved 30th July 2018, <https://data.amsterdam.nl>
- City of Amsterdam, "Policy: City in Balance", City of Amsterdam [website], retrieved 10th January 2019, available here: <https://www.amsterdam.nl/en/policy/policy-city-balance/>
- Cloin, Cindy, "Assen moves to utopia 'Sensor City'", *Trouw*, January 7th, 2017, <https://www.trouw.nl/home/assen-vertilt-zich-aan-utopie-sensor-city~a2638a3b/>
- Crawford, K., "The Hidden Biases in Big Data" [WWW Document], *Harvard Business Review*, 2013, available at: <https://hbr.org/2013/04/the-hidden-biases-in-big-data> (accessed 1.4.17).
- Devi, Suguna, T. Neetha, "Machine Learning Based Traffic Congestion Prediction in a IoT Based Smart City", *IRJET*, Vol. 4, Issue 5, 2017, pp. 3442-3445.
- Elmaghraby, Adel S., and Michael M. Losavio, "Cyber Security Challenges in Smart Cities: Safety, Security and Privacy", *Journal of Advanced Research*, Vol. 5, Issue 4, 2014, pp. 491-497.
- Fitzgerald, Michael, "Data-Driven City Management: A Close Look at Amsterdam's Smart City Initiative", *Sloan Review*, May 19th, 2016, <https://sloanreview.mit.edu/case-study/data-driven-city-management/>
- Galdon-Clavell, Gemma, "(Not So) Smart Cities? The Drivers, Impact and Risks of Surveillance-Enabled Smart Environments", *Science and Public Policy*, Vol. 40, 2013, p. pp. 717-723.
- Gemeente Amsterdam, "Availability and Quality of Data", *Gemeente Amsterdam* [website], retrieved 30th July 2018, 2018a, <https://data.amsterdam.nl/#?mpb=topografie&mpz=11&mpv=52.3731081:4.8932945&pgn=content-detail&pgi=item1&pgt=beleid>
- Gemeente Amsterdam, "Vragen en antwoorden over Amsterdam City Data", *Gemeente Amsterdam* [website], retrieved 30th July 2018, 2018b, <https://data.amsterdam.nl>
- Glaeser, Edward L., Scott Duke Kominers, Michael Luca, and Nikhil Naik, "Big Data and Big Cities: The Promises and Limitations of Improved Measures of Urban Life", *Economic Inquiry*, Vol. 56, Issue 1, 2018, pp. 114-137.
- Glasmeier, Amy, and Susan Christopherson, "Thinking About Smart Cities", *Cambridge Journal of Regions, Economy and Society*, Vol. 8, 2015, pp. 3-12.
- Grashoff, Wimfred, "Businesscase DataPunt", *Gemeente Amsterdam* [website], 21st June 2017, 2017a, https://assets.amsterdam.nl/publish/pages/841982/buca_DataPunt_v1_0_20170621_voor_publicatie.pdf

- Grashoff, Wimfred, "Privacy en Beveiliging in DataPunt", *Gemeente Amsterdam*, 21st June 2017, 2017b, https://assets.amsterdam.nl/publish/pages/841982/20170621_privacy_en_informatiebeveiliging_DataPunt_pub.pdf
- Hashem, Ibrahim Abaker Targio, Victor Chang, Nor Badrul Anuar, Kayode Adewole, Ibrar Yaqoob, Abdullah Gani, Ejaz Ahmed, and Haruna Chiroma, "The Role of Big Data in Smart City", *International Journal of Information Management*, Vol. 36, Issue 5, 2016, pp. 748-758.
- Hein, Anton, "Amsterdam Europe's Eight Most Popular City Destination", *Dutch Amsterdam* [website], February 2nd, 2016, <http://www.dutchamsterdam.nl/4456-amsterdam-europe-eight-most-popular-city-destination>
- Hollands, Robert G. "Critical Interventions into the Corporate Smart City", *Cambridge Journal of Regions, Economy and Society*, Vol. 8, Issue 1, 2015, pp. 61-77.
- Kitchin, Rob, "Big Data and Human Geography: Opportunities, Challenges and Risks", *Dialogues in Human Geography*, Vol. 3, Issue 3, 2013, pp. 262-267.
- Kitchin, Rob, "Data-Driven Networked Urbanism", *The Programmable City Working Paper 14*, 10th August 2015, 2015a.
- Kitchin, Rob, "Getting Smarter about Smart Cities: Improving Data Privacy and Data Security", *Data Protection Unit*, Department of the Taoiseach, Dublin, Ireland, 2016a.
- Kitchin, Rob, "Making Sense of Smart Cities: Addressing Present Shortcomings", *Cambridge Journal of Regions, Economy and Society*, Vol. 8, 2014, pp. 131-136.
- Kitchin, Rob, "Reframing, Reimagining and Remaking Smart Cities", *The Programmable City Working Paper 20*, 16th August 2016, 2016b.
- Kitchin, Rob, "The Ethics of Smart Cities and Urban Science", *Phil. Trans. R. Soc. A*, Vol. 374, 2016c, pp. 1-15.
- Kitchin, Rob, "The Promise and Perils of Smart Cities", *Society for Computers & Law*, Vol. 26, Issue 2, 2015b, pp. 1-5.
- Kitchin, Rob, "The Real-Time City? Big Data and Smart Urbanism", *GeoJournal*, Vol. 79, 2014, pp. 1-14.
- Kitchin, Rob, "The Realtime-ness of Smart Cities", *TECNOSCIENZA: Italian Journal of Science & Technology Studies*, Vol. 8, Issue 2, 2018, pp. 19-42.
- Kitchin, Rob, Claudio Coletta, Leighton Evans, Liam Heaphy and Darach Mac Donncha, "Smart Cities, Urban Technocrats, Epistemic Communities and Advocacy Coalitions", *The Programmable City Working Paper 26*, 8th March 2017, 2017.
- Kitchin, Rob, Tracey P. Lauriault, and Gavin McArdle, "Smart Cities and the Politics of Urban Data", *Smart Urbanism: Utopian Vision or False Dawn?* Routledge, London, 2015, pp. 16-33. ISBN 9781138844223.
- Interviewee 1, "Interview", November 6th, 2018.
- Li, DeRen, JianJun Cao, and Yuan Yao, "Big Data in Smart Cities", *Science China Information Sciences*, Vol. 58, Issue 10, 2015, pp. 1-12.

- Li, Yibin, Wenyun Dai, Zhong Ming, and Meikang Qiu, "Privacy Protection for Preventing Data Over-Collection in Smart City", *IEEE Transactions on Computers*, Vol. 65, Issue 5, 2016, pp. 1339-1350.
- Martínez-Ballesté, Antoni, Pablo A. Pérez-Martínez, and Agusti Solanas, "The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City is Possible", *IEEE Communications Magazine*, Vol. 51, Issue 6, 2013, pp. 136-141.
- Moerman, Marcel, "Projectstartarchitectuur: DataPunt", *Gemeente Amsterdam* [website], 21st March 2017, https://assets.amsterdam.nl/publish/pages/841982/20170626_DataPunt_psa_v1_0.pdf
- Municipality of Amsterdam, "Launch of Amsterdam City Data: A Wealth of Data about the City", *Municipality of Amsterdam* [website], 30th July 2018, <https://www.amsterdam.nl/bestuur-organisatie/organisatie/overige/stad-vol-data/actueel-data/lancering-acd/>
- Naafs, Saskia, "'Living Laboratories': The Dutch Cities Amassing Data on Oblivious Residents", *The Guardian*, March 1st, 2018, 2018, <https://www.theguardian.com/cities/2018/mar/01/smart-cities-data-privacy-eindhoven-utrecht>
- Nam, Taewoo, and Theresa A. Pardo, "Smart City as Urban Innovation: Focusing on Management, Policy, and Context", *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, ACM, 2011, pp. 185-194.
- Nigon, Julien, Estèle Glize, David Dupas, Fabrice Crasnier, Jérémy Boes, "Use Cases of Pervasive Artificial Intelligence for Smart Cities Challenges", *IEEE Workshop on Smart and Sustainable City (WSSC 2016) associated to the International Conference IEEE UIC 2016*, Toulouse, France, July 2016.
- Pan, Yunhe, Yun Tian, Xiaolong Liu, Dedao Gu, and Gang Hua, "Urban Big Data and the Development of City Intelligence", *Engineering*, Vol. 2, Issue 2, 2016, pp. 171-178.
- Pieters, Janene, "Tourism in the Netherlands up 9 Percent; Biggest Increase in 12 Years", April 4th, 2018, *NL Times* [website], <https://nltimes.nl/2018/04/04/tourism-netherlands-9-percent-biggest-increase-12-years>
- Rjab, Amal Ben, and Sehl Mellouli, "Smart Cities in the Era of Artificial Intelligence and Internet of Things: Literature Review from 1990 to 2017", *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, May 30-June 1, 2018, Delft, Netherlands, ACM, 2018.
- Scrum Values & Agile Methodologies for Project Management [WWW Document], 2018, available here: <https://www.scrumalliance.org/learn-about-scrum/scrums-values>
- Sen, Mourjo, Anuvabh Dutt, Shalabh Agarwal, and Asoke Nath, "Issues of Privacy and Security in the Role of Software in Smart Cities", *International Conference on Communication Systems and Network Technologies (CSNT)*, 2013, pp. 518-523.
- The Seven Foundational Principles [WWW Document], Ryerson University. 2018, URL <https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/>
- Sholla, Sahil, Roohie Naaz, and Mohammad Ahsan Chishti. "Ethics Aware Object-Oriented Smart City Architecture", *China Communications*, Vol. 14, Issue 5, 2017, pp. 160-173.

- Srivastava, Shweta, Aditya Bisht, and Neetu Narayan, "Safety and security in smart cities using artificial intelligence—A review", *Data Science & Engineering-Confluence, 2017 7th International Conference on Cloud Computing*, IEEE, 2017, pp. 130-133.
- van Zoonen, Liesbet, "Privacy Concerns in Smart Cities", *Government Information Quarterly*, Vol. 33, Issue 3, 2016, pp. 472-480.
- Vázquez Salceda, Javier, Sergio Álvarez Napagao, José Arturo Tejeda Gómez, Luis Javier Oliva Felipe, Dario Garcia Gasulla, Ignasi Gómez Sebastià, and Víctor Codina Busquet, "Making Smart Cities Smarter Using Artificial Intelligence Techniques for Smarter Mobility", *SMARTGREENS 2014: proceedings of the 3rd International Conference on Smart Grids and Green IT Systems*, SciTePress, 2014, pp. IS7-IS11.
- Yin, ChuanTao, Zhang Xiong, Hui Chen, JingYuan Wang, Daven Cooper, and Bertrand David, "A Literature Survey on Smart Cities", *Science China Information Sciences*, Vol. 58, Issue 10, 2015, pp. 1-18.
- Zanella, Andrea, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi, "Internet of Things for Smart Cities", *IEEE Internet of Things Journal*, Vol. 1, Issue 1, 2014, pp. 22-32.
- Zhang, Kuan, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin Sherman Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions", *IEEE Communications Magazine*, Vol. 55, Issue 1, 2017, pp. 122-129.

CS03 – Agriculture



Ethics of Using AI and Big Data in Agriculture: The Case of BASF



This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641



Document Control

Deliverable	Deliverable 1.1.: Case Studies
WP/Task Related	WP 1: Representation and Visualisation
Delivery Date	Date Deliverable Due 31/1/2019
Dissemination Level	Public
Lead Partner	Partner Name
Contributors	Mark Ryan, University of Twente
Reviewers	Kevin Macnish, Bernd Stahl, Doris Schroeder
Abstract	
Key Words	

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes
1.1	13/12/2018	Mark Ryan	Kevin Macnish	
1.2.	10/01/2019	Mark Ryan	Doris Schroeder	
1.3	25/01/2019	Mark Ryan		

Contents

Executive Summary	87
Agricultural SIS and Ethics: A Case Study	88
1. The Use of SIS in Agriculture	89
2. Ethical Issues of Using SIS in Agriculture	91
2.1. Accuracy of Data and Recommendations	92
2.2. Data Ownership and Intellectual Property	92
2.3 Economic Issues and the Digital Divide	93
2.4. Privacy and Security	94
2.5. Animal Welfare and Environmental Protection	95
3. BASF: The Case of a Large Multinational Company Using SIS in Agriculture	95
3.1. BASF and the Interviewees	96
3.2. SIS Technologies at BASF	96
3.3. Potential Technical Challenges of Using SIS for BASF	98
3.4. Feedback from Stakeholders	99
4. BASF: Ethical Issues from SIS Technology	100
4.1. Accuracy of Data and Recommendations	100
4.2. Data Ownership and Intellectual Property	101
4.3 Economic Issues and the Digital Divide	102
4.4. Privacy and Security	102
4.5. Environmental Protection	103
4.6. Employment	103
5. Conclusion	104
5.1. Limitations	104
5.2. Contribution to Knowledge	105
5.3. Implications of this Report	105
5.4. Further Research	106
6. References	106

Executive Summary

Smart information systems (Big Data and artificial intelligence) are used in the **agricultural industry** to help the planting, seeding, and harvesting of crops, as well as farm management, plant and livestock illness and disease detection. I looked at how the **Crop Protection Division at BASF** is using smart information systems (SIS), through their **Maglis project**, to provide farmers with local weather predictions, farm efficiency and sustainability metrics, and early detection systems for weed, pests and disease. SIS being used in agriculture, types of data retrieved from the farm, how this data is analysed, and agribusinesses involved in this burgeoning field. Agricultural SIS has the potential to **automate activities** that are typically done by agronomists, allowing for cost reductions, quick and effective crop forecasting, and improved decision-making and efficiency for the farmer. Agricultural SIS also offers agribusinesses an additional revenue, better customer-relations, and reduced costs from hiring additional agronomists and advisors.

The world's population will exceed 9 billion by 2050, forcing the agricultural sector to increase its production levels by up to 70%. SIS are being hailed as one possible solution to help plant, seed, harvest, and manage farms better and more effectively. However, the use of agricultural SIS may create a number of ethical concerns. For example, the **accuracy of data and recommendations** provided by SIS may lead to lost harvests, ill livestock, and loss of earnings. There is also a tension between ensuring an agribusinesses' **intellectual property** and the protection of the farmer's **data ownership**. The use of SIS is relatively expensive, which may create a **digital divide**. Agricultural Big Data is also vulnerable to **privacy and security** threats because it could be used nefariously by corrupt governments, competitors, or even market traders. Sensors, robots and devices may cause harm, distress, and damage to **animal welfare and the environment**.

To assess if these ethical issues mirror those experienced in the field, I interviewed three members of BASF working on their SIS project 'Maglis', launched in 2016. Maglis combines data retrieved from the farmer with BASF's agronomic knowledge to **manage their farm more effectively**. Maglis was designed to provide farmers with local weather predictions, plant disease in situ detection, and recommendation tools to minimise risk, crop and yield previews, farm efficiency and sustainability metrics, and early detection systems for weed, pests and disease. One of the primary motivations for using SIS technology for BASF is the ability to make the farmer's life easier, more productive, and to **save costs**. The aim is to improve farm management, not by increasing fertilizer use, but by more intelligent farming decisions and practices.

The ethical issues faced in the Maglis project strongly correlated with those in the literature, with the addition of **employment**. The general public is concerned that SIS will replace human jobs, such as the agronomist, but the BASF team stated that their SIS is intended to complement the human expert, rather than replace them. **Accuracy and availability of data** proved to be an issue because not all farmers had available data and data retrieved from third-parties may not be accurate. The Maglis team ensure that their customers' **privacy** is protected by having strong **security** measures to avoid misuse and hacking. **Data ownership** belongs to the farmer and they can move to a different farm management system supplier, with that data, if they choose to. Maglis is free to use to avoid the issue of a **digital divide**. BASF incorporate a strong **sustainability** agenda into their SIS, developing it from the European PEF (Product Environmental Footprint) and the company's Life-cycle assessment (LCA) frameworks. Overall, my report was able to evaluate how ethical issues found within the SIS literature correlate with those identified, and tackled, in practice.

Agricultural SIS and Ethics: A Case Study

Approximately 26.5% of the world's population work in agriculture, which accounts for nearly \$3 trillion in global trade (The World Bank 2018). Despite this, it is an industry that needs to grow its production levels by 70% to feed the world's growing population by 2050 (Schönfeld, Heil and Bittner 2016; Kamilaris, Kartakoullis, and Prenafeta-Boldú 2017). In addition, our current ecological footprint is twice the level that it should be; leaving the agricultural sector with the colossal challenge of producing more food, while reducing their ecological impact (Popa 2011; Wolfert, Sørensen, and Goense 2014).

The agricultural industry is looking at different solutions to meet these challenges, one of which is data analytics. Big Data analytics is seen as the fourth technological revolution in agriculture and it is hoped that it will provide a solution to our growing food demands (Kumari, Bargavi and Subhashini 2016; Morota et al. 2018; O'Grady and O'Hare 2017).²⁴

It is predicted that Big Data analytics will take on a fundamental role in the future of agriculture (Zhang et al 2014; Carolan 2015). Agricultural Big Data, data analytics, and machine-learning algorithms are the catalysts that are expected to underpin the realisation of the world's agricultural goals.

Agricultural Big Data analytics is the analysis of large datasets from a wide range of resources, often using artificial intelligence (AI) techniques. The integration of Big Data and AI (Smart Information Systems - SIS) is expected to be vital for the successful growth of the agricultural sector. Agribusinesses are now shifting their focus towards data-driven agricultural solutions. While these developments are seen as effective ways to achieve the challenging goals ahead, they also raise a number of serious social and ethical concerns that we will analyse in this case study.

The primary research questions are: Which ethical issues arise in the use of SIS in agriculture? And how can they be addressed?

The primary research questions that will be addressed in this case study report are: Which ethical issues arise in the use of SIS in agriculture? And how can they be addressed? To answer the questions, the key issues within the literature on the topic will be analysed and interviews with three staff members working for a large multinational agricultural organisation – BASF, will be conducted.

The aim of this case study is to identify ethical issues that may appear in practice in an agricultural organisation that are not covered in the literature; whether or not they face the same issues discussed in literature as in practice; and if there are policies and procedures set in place for addressing these concerns.

The case study will be divided into four main sections, with the first two sections focusing on an analysis of the literature in the field, while sections three and four focus on the organisation BASF. Section 1 will analyse the current implementation of agricultural data analytics and establish how SIS technology is used in practice; while section 2 will concentrate on a range of social and ethical issues surrounding SIS use and implementation in the agricultural sector. Section 3 will analyse an organisation using agricultural SIS technologies: the large multinational chemical company BASF. Section 4 will critically evaluate ethical issues that arise when using SIS technologies in BASF, incorporating the three interviews done at BASF (Limburgerhof, Germany) on August 22nd, 2018.

²⁴ The industrial revolution, the green revolution, and the biotechnology revolution.

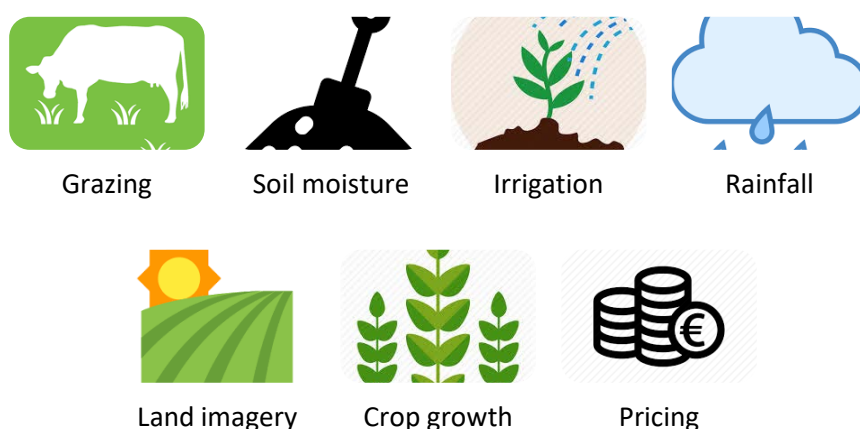
1. The Use of SIS in Agriculture

Before analysing the social and ethical issues that may arise from using SIS technology in the agricultural sector, it is important to understand how and why these technologies are being developed in the first place. In order to effectively understand the societal and ethical implications of using such technologies, it is vital to elaborate on the types of data being retrieved, where they are being retrieved from, and how are they being applied.

This section will focus on the use of SIS in the agricultural sector in order to elucidate the different ways these technologies are used in practice and by whom, i.e. who are the companies developing them. An extensive literature review was conducted of the different ways that agricultural SIS technology is used and implemented, and on a number of agribusinesses integrating SIS within their business models in order to demonstrate how they are being incorporated in practice. The review ranged from computer science, agricultural management, and agricultural practice, to agricultural Big Data literature, in order to establish an exhaustive overview of the different stages of agricultural SIS technology's use and application.

To begin with, there are many different components in agricultural SIS integration, from the retrieval, analysis and prescription of data. The *types* of data retrieved range from: animal movement and grazing patterns, soil moisture and nutrient level, irrigation, rainfall and climate, land imagery, crop growth patterns, and market pricing (Bennett 2015; Kamilaris, Kartakoullis, and Prenafeta-Boldú, 2017).

Figure 1 – Types of Agricultural Data Retrieved



This data is retrieved from many different *sources*: weather stations, surveys, static historical datasets, geospatial data, satellite imagery, farm sensors, farm equipment sensors, radiation sensors, climate sensors, and GPS-based field maps (Tzounis et al. 2017; and Ribarics 2016). The data is also applied in a number of different contexts: weather and climate, land, animal research, crops, soil, weeds, food availability and security, biodiversity, and farmers' insurance and finance (Kamilaris, Kartakoullis, and Prenafeta-Boldú, 2017).

Despite the potential value of applying agricultural Big Data in all of these contexts, the amount of data that is currently being analysed is still relatively small (Hirafuji 2014). This is set to grow rapidly because of the abundance of *benefits* promised by the effective use of agricultural Big Data. These include: improve water and air quality, improved soil health, food quality and security, protection of biodiversity, improvements to quality of life, increase output, cost reductions, crop

forecasting, and improved decision-making and efficiency (Castle, Lubben, and Luck 2015, Mintert et al. 2016, O’Grady and O’Hare 2017, Schönfeld, Heil and Bittner 2016, and Sonka and Cheng 2015).

Figure 2 – Promised Areas of Improvements of Agriculture by Data²⁵



It is argued that SIS can help during the planting stage to maximise crop yields, or to react to diseases, animal ill-health, or unfavourable climatic conditions. SIS can also assist farmers in managing their farms through effective ‘prescriptive farming’ (Antle, Capalbo and Houston, 2015). Therefore, many propose that ‘good farmers do not follow their gut, they follow data’ (Carolan 2015, p. 11).

Many propose that ‘good farmers do not follow their gut, they follow data’.

Monsanto estimate that data analytics will increase global crop production by \$20 billion annually (Bunge 2014). Therefore, traditional agricultural businesses (e.g. machinery, seed or chemical companies) have branched out into data analytics, to become agricultural technology providers (ATPs). They sell prescriptive analytics to farmers: ‘The farmer generates (or hires the dealer or a third-party company to generate) data on field-specific attributes such as GPS-coded soil sampling and field maps for selected plots of land’ (Sykuta 2016, p. 60). Using different machine-learning algorithms and data analytics software, along with a wide-range of the company’s datasets and acquired datasets, the farmer’s data is transformed into prescriptive recommendations by ATPs.

There are many different agricultural companies implementing SIS technology in their programs. For example, Monsanto’s FieldScripts® program retrieves data from the farmer and combines it with Monsanto’s agronomic knowledge and prescribes recommendations to the farmer. ‘The dealer and Monsanto’s field agents help monitor performance through the season and advise on field management needs. At the end of the season, the farmer submits yield data to help improve future prescriptions for the field, which Monsanto can incorporate to update its basic algorithm as well’ (Sykuta 2016, p. 61).

DuPont Pioneer’s Field360™ and WinField R7 programs identify hybrid seed selection, provide crop management projections and crop growth estimations, and recommend planting methods (Sykuta 2016, p. 61). Pioneer’s Field360™ Select Software ‘combines current and historical field data with real-time agronomic and weather information to help growers make informed management decisions’ (Antle, Capalbo and Houston, 2015, p. 3).

²⁵ Cost reductions, crop forecasting, and improved decision-making and efficiency are additional promised benefits directly for farmers.

John Deere attaches sensors to its farming equipment and analyses the data collected from them, then sells recommendations back to farmers (Bronson and Knezevic, 2016). John Deere's analytics service costs farmers \$15 per acre of farmland but promises a \$100 per acre increase in profits. 'This programme gives users access to algorithms that show historical trends of soil moisture and crop level weather patterns going back 30 years. The product allows farmers to plug in different seeds and receive as output, before planting season has even commenced, what their likely yields will be that fall' (Carolan 2015).

John Deere's analytics service costs farmers \$15 per acre of farmland but promises a \$100 per acre increase in profits.

The integration of data analytics is often intertwined with traditional agricultural business models, for example, the seed business for Monsanto and DuPont Pioneer, and tractor business for John Deere. Many of the most notable agribusinesses are driving towards an adoption of the "smart farm" framework, fully technologised with a constant retention and application of data (Coble et al. 2018).

There are many pressing social and ethical concerns in the literature relating to the implementation of smart information systems within the agricultural domain. It is important to analyse these in order to identify which ethical issues arise in the use of SIS in agriculture and how they can be addressed. It is also important to identify these issues for comparative purposes with the issues highlighted in the interviews with the three members of BASF, later in this report.

2. Ethical Issues of Using SIS in Agriculture

In the key journals on agricultural and environmental ethics, there was no research published on the ethics of SIS in the agricultural industry. These journals included 'Agriculture and Human Values', 'Journal of Agricultural Ethics', 'Journal of Agricultural and Environmental Ethics'. 'Environmental Values', 'Environmental Ethics', and 'Ethics, Policy, and Environment'.

A broad keyword search, using multiple different variations, was therefore conducted to attract relevant articles, achieved by collating literature from bibliographical databases: Google Scholar, ScienceDirect, Web of Science and Scopus. Using this approach, the following issues were identified: accuracy of data and recommendations provided from algorithms; data ownership; digital divide, privacy and security; and animal welfare and environmental protection.

Figure 3 – Ethical Issues in the Literature – SIS & Agriculture



2.1. Accuracy of Data and Recommendations

The primary purpose of integrating SIS technologies within the agricultural sector is to enable better decisions, adaptation to circumstances and prescriptions (Talavera et al. 2017). However, some claim that machine learning is not fit for purpose because the algorithms used are only suitable for small datasets (Zhang et al. 2014). These algorithms cannot effectively analyse Big Data or large datasets because of their inability ‘to strike a balance between timeliness and accuracy of processing’ (Zhang et al., 2014, p. 141). This is a technical limitation that needs to be addressed within the agricultural sector, and more broadly, the SIS industry as a whole. Limited data may also create misleading conclusions. ATPs may provide prescriptive recommendations that cause detrimental outcomes, which are based on incorrect or inaccurate data (Taylor and Broeder 2015, p. 13).

There is also a possibility that the retrieval of data is misleading or inaccurate because of environmental circumstances. For example, animals may interfere with SIS technologies by affecting the radio signals used to communicate by being too close to sensors or interfering with the equipment (O’Grady and O’Hare 2017). Sensors can be shielded against damage, but there are also concerns regarding circumstances that give false readings, such as temperature extremes and humidity (Tzounis et al. 2017). Possible interferences need to be considered to minimise false readings, skewed analytics and misleading prescriptions.

Another potential issue is that data may be difficult to interpret because of local differences or idiosyncrasies (Byarugaba Agaba et al. 2014, p. 21). Therefore, there is a clear need to analyse data contextually to make unbiased decisions (Taylor et al. 2014). If these differences are not factored into the prescriptive analysis, it may lead to lost resources and harm to the farmer’s livelihood. ATPs also need to be confident in the accuracy and legitimacy of information provided by farmers in order to provide appropriate recommendations (Lokers et al. 2016). While the accuracy of data and recommendations are not ethical issues in themselves, providing inaccurate data to farmers or giving inaccurate recommendations may lead to lost harvests, ill livestock, and loss of earnings and negative impacts on their business.

2.2. Data Ownership and Intellectual Property

There are concerns about distribution of farm data to third parties (Rosenheim and Gratton 2017, p. 403). Farmers fear that their data may end up in the wrong hands and subsequently be used against them (Ferris 2017). Some farmers worry that if they surrender their data, it will put them in a precarious position in the future (Coble et al. 2018, p. 84). They are concerned about the collection and dissemination of their data to regulatory bodies, agencies and governmental officials (Sykuta 2016). Their data may be used against them in a wide array of different contexts, such as regulatory enforcement, imposition of charges, fees, fines, and restrictions. There is also the concern that their data will be used by commodity traders on the stock market (Ferris 2017). This could be used against farmers by finding out specific information about the farm that would allow traders to purchase it for less, or be used as a bargaining chip against the farmer.

Who owns the data and who can monetize the data?

Therefore, one of the most contentious issues relating to SIS implementation is regarding data ownership (Schönfeld, Heil and Bittner 2016). Essentially, ‘who owns the data and who can monetize [the data]’ (Kamilaris, Kartakoullis, and Prenafeta-Boldú, 2017, p. 29). The issue of data ownership raises the question ‘whether farms should relinquish control of farm data to third parties’ (Coble et al. 2018, p. 84). There is the concern that farmers’ data will be used to sell unnecessary products back to them (Ferris 2017). ‘Big

agricultural firms such as Monsanto might influence farmers to buy specific seeds, sprays, and equipment and are likely to profit from the costs of their service and higher seed sales' (Ksetri 2014, p. 13). There appears to be an opacity about who owns the data retrieved from farms and who has control over their use and implementation (Kosier 2017).

Many ATPs insist that farmers own their data, but the ATPs may include a royalty-free license over these data, so they can be used by the ATP regardless of ownership (Darr 2014). If farmers own their data, and they want to change to a different ATP, they may be in breach of contract. For example, Monsanto have tight legislative controls over their intellectual property and data analytics, and if a farmer breaches their contract, this may lead to penalties and/or court-cases against them. Furthermore, if a farmer is looking for a different ATP, it may be difficult or even impossible to find another ATP because of data ownership issues: 'ATPs may have concerns about receiving data from farmers that the farmer herself does not own, giving rise to potential violations of intellectual property or licensing restrictions' (Sykuta 2016, p. 66).

ATPs have tight legislative controls over their intellectual property and data analytics, and if a farmer breaches their contract, this may lead to penalties and/or court-cases against them.

Fundamentally, ATPs need to protect their intellectual property rights and investments in SIS. One way to ensure this is through contractual agreements with farmers. However, in the United States 'fewer than seven percent of small-scale and medium-scale farms used contracts while over 50 percent of very large farms used contracts' (Sykuta 2013, p. 19). The use of SIS technologies may force smaller farmers into contractual obligations with ATPs. Many of these farmers have no experience with legal documents and contractual terminology, so there is the possibility that farmers will not understand what they are consenting to when using SIS, raising ethical issues around sufficient informed consent to enter into these agreements. In addition to this lack of knowledge about legal descriptions, there is also the concern that the technologies themselves are beyond the average farmer's capacity.

Data retrieved from farms is often inaccessible to farmers themselves, with many fearing that they do not have the technological capacity to use SIS (Sykuta 2016, p. 60). Technical knowledge is required to interpret this data, and farmers may not be able to get this knowledge for free, and so become dependent on ATPs (Schönfeld, Heil and Bittner 2016). There is also the possibility that the role of farmers will be reduced, and a lot of associated freedoms curtailed, because of data analytics (Wolfert et al. 2017). Farmers have already started to see restrictions imposed on their land and farm machinery. Companies such as John Deere have implemented policies that disallow farmers repairing or fixing their own machinery, as this may infringe upon copyright and intellectual property given that the company's hardware is contained on/within the vehicle. Any tampering with these devices is hence a breach of contract, and subjugated to economic penalties (Carolan 2015).

2.3 Economic Issues and the Digital Divide

Small farms far exceed the number of large farms globally. In the United States alone, 66% of all farms do not exceed \$1 million in annual sales (USDA NASS, 2014). In LMICs (low-to-middle-income countries), most agriculture occurs on small farms with very little technology. However, most agricultural data analytics is only being done on large monoculture industrial farms (Carbonell 2016). This may cause an issue of disproportionate growth of larger farms and the potential dissolution of smaller farms. The use of SIS technologies is relatively expensive, which may also prevent poorer farmers from adopting them (Kosier 2017, p. 11, Schönfeld, Heil and Bittner 2016). This leads to a 'digital divide' between those who can implement SIS and those who cannot (Kamilaris, Kartakoullis,

and Prenafeta-Boldú, 2017, p. 29). Rural remote locations may also suffer from data transmission limitations, which could prevent farmers from using these technologies. SIS technologies hence have the potential to create or exacerbate inequalities between those who can use them and those who cannot (Poppe, Wolfert and Verdouw 2014).

The agricultural sector is the largest employer in LMICs and requires substantial growth in the coming years to meet increasing food demands. In these countries, yields are often reduced by up to 40% because of poor farming techniques, lack of information and incorrect planting, weeding and harvesting times (Ksetri 2014, p. 10). Therefore, one of the biggest areas of potential for SIS is in LMIC countries (Ksetri 2014). There is hence a push towards transforming unstructured data into implementable goals for LMIC development (Global Pulse 2012, Panicker 2013) and the UN has proposed that significant development in LMICs will be the result of effective data analytics and the implementation of their results (Micheni 2015). However, there are many obstacles impeding SIS adoption in LMICs, such as the lack of technical capabilities to analyse and formulate this data in lower tech countries, lack of investment, poor technological infrastructure, and political and economic instability (Micheni 2015). Furthermore, privacy and data protection laws are quite scarce or non-existent in many LMICs, so the collection and processing of data remain essentially unregulated (Taylor and Broeder 2015, p. 15).

2.4. Privacy and Security

Even though information about individuals could potentially be anonymised, Big Data in agriculture may still lead to negative repercussions for groups of people. Authorities and corporations can draw conclusions and implement courses of action at a group level, for instance, which may be undesirable for farmers. Essentially, 'it is precisely being identified as part of a group which may make individuals most vulnerable, since a broad sweep is harder to avoid than individual targeting' (Taylor 2017). This is particularly pertinent in LMICs, where there is less data protection regulation. For example, in sub-Saharan Africa, only 8 out of the 55 countries have data protection legislation (Taylor 2017). In the agricultural sector, this data could be used nefariously by corrupt governments, competitors, or even market traders.

At present, there is very little regulation on agricultural data (Ferris 2017). It is claimed that Big Data in the agricultural sector is not as vulnerable to privacy and security concerns as other sectors (Zhang et al. 2014). This is because ATPs do not collect obviously sensitive data, such as information about children, banking data, or healthcare records (Ferris 2017). Despite this, farmers still provide a wide range of details about their farm. Personal information relating to names, locations, property types, income levels and valuations are retrieved for processing (Ferris 2017). These are all personal data, some highly sensitive, e.g. income. There is also a concern that drones, and other data-retrieving technologies, will monitor third-party individuals, infringing upon their personal privacy (Schönfeld, Heil and Bittner 2016).

At present, there is very little regulation on agricultural data.

Big Data is retrieved from many different sources, such as radio equipment, agricultural information websites and mobile terminals (Zhang et al. 2014). As a result, there are a multitude of potentially sensitive data types that need to be stored and transferred, so data security is a very important concern for farmers (Tzounis et al. 2017). Farmers need to be assured that their data are safe, used appropriately and interpreted in the correct manner (Lokers et al., 2016). However, this is difficult to universalise because the 'nature of data security issues also differ by vendor given their services and platforms' (Sykuta 2016, p. 60). Also, the type of data that is retrieved varies in terms of

security needs, for example, securing data about a farmer's sales and yields may be far more sensitive than data about rainfall levels on the farm.

2.5. Animal Welfare and Environmental Protection

The implementation of sensors, robots and other devices on farms may cause undue stress or harm to farm animals and external wildlife. These electronic devices and sensors may upset, injure or even kill livestock and/or local wildlife. Robots, sensors and unmanned aerial vehicles (UAVs) also have the potential to emit toxic material, fumes and waste into their surrounding environment. An additional concern is that the algorithmic prescriptions used by such devices may cause detrimental effects because they do not consider land external to the farm (Antle, Capalbo and Houston, 2015). For example, some potential effects could be surface water run-off, encroachment on habitats, or general pollution to the surrounding area. Therefore, the ecological and social effects of implementing and deploying SIS technologies to the wider environment are significant factors (Kosier 2017).

After discussion the many ethical issues covered in the literature that are related to the use of SIS in the agricultural industry, it is evident that these concerns cover a broad spectrum of issues. In order to better understand the ways in which these issues arise in practice, the following section will describe a specific case of agricultural SIS. The case was chosen because BASF is the largest chemical producer in the world and is quickly becoming a leading competitor in the agricultural industry in Europe. Along with that, it is one of only a few leading agribusinesses that is investing in the development of agricultural SIS. Many of the companies developing agricultural SIS are based in the US (Monsanto, DuPont Pioneer, and John Deere), which would veer away from the aims of the European-focused SHERPA project. All of these factors made BASF the leading choice in companies to conduct a case study on.

3. BASF: The Case of a Large Multinational Company Using SIS in Agriculture

BASF implements and uses SIS technology within the agricultural sector. Three interviews were conducted with BASF staff members. During these interviews, their interactions with SIS and what they view as some of the most fundamental issues pertaining to this technology were discussed. The interviews were conducted on August 22nd, 2018 at BASF Crop Division Headquarters in Limburgerhof, Germany.

The three interviewees were Interviewee 1, Interviewee 2, and Interviewee 3 working in BASF. The interviews were transcribed a month later and evaluated in early October. A qualitative analytics software tool (NVIVO) was used in order to categorise, define, and evaluate the content of the three interviews. Topics were split into different nodes during a two-day SHERPA consortium workshop to evaluate 11 SHERPA case studies. A range of sections pertinent to SIS technology was established. The interviews conducted at BASF were then segmented and categorised within these nodes, which were analysed to produce this report.

Table 1 *BASF Interviewees Working on SIS Technology*

BASF Interviewees Working on SIS (Maglis Project)			
Interviewee	Interviewee 1	Interviewee 2	Interviewee 3
Role in Organisation	Global Governmental Affairs & Management	Sustainability	Foundation Division

Length of Interview	40 minutes	35 minutes	55 minutes
----------------------------	------------	------------	------------

3.1. BASF and the Interviewees

In 2016, BASF generated sales of €58 billion, of which \$5.6 billion was from the Crop Protection Division. BASF finalised the acquisition of the \$5.9 billion Bayer herbicide and seed business in 2018 (BASF 2017c). Part of this acquisition is a range of data compiled by Bayer. In 2017, BASF were very active in data acquisitions and partnerships: They entered a satellite data-sharing partnership with the European Space Agency, a development and operations agreement with the data insights company Proagrica, and they acquired the agricultural business intelligence systems specialist ZedX Inc. (BASF 2017a, BASF 2017b, ZedX Inc., 2017a, and ZedX Inc. 2017b). BASF has traditionally been a large multinational chemical company, but over the past decade has grown its Crop Protection Division and data analytics business, such as the Maglis platform.

The interviewees from BASF Crop Protection Division were Interviewee 1, who works in Global Governmental Affairs and Issue Management; Interviewee 2, who works on the sustainability component of Maglis; and Interviewee 3 working on the backend running of Maglis. Interviewee 1's role focuses on the advocacy of digital initiatives in the company and ensuring communication with different stakeholders, such as policymakers and governmental bodies. Interviewee 2 is

'the architect of algorithms which translate farming practices into sustainability language, and then back into, hopefully, improving farming practices' (Interviewee 2).

The Interviewee 3 who was interviewed works in the Foundation division of Maglis, ensuring the functionality and usability of the backend systems of the project, such as user management systems, managing users.

3.2. SIS Technologies at BASF

BASF's data analytics company Maglis™ was launched in 2016 to provide farmers with a range of crop management options within one comprehensive platform (BASF 2016, Infosys 2018).²⁶ The Maglis project started in Canada and was launched subsequently in the UK. It is currently in the process of being launched in Germany. Maglis is intended to complement the BASF Grow Smart programme, by personalising the exact purchase needs of farmers.²⁷ BASF are collaborating with the tech company Infosys, and they have also entered a three-year partnership with ZedX Inc., to work on the Maglis project (Bedford 2017). ZedX Inc. retrieves weather conditions, wind speeds, crop protection, and pest and agronomic data. It then analyses these data to produce effective

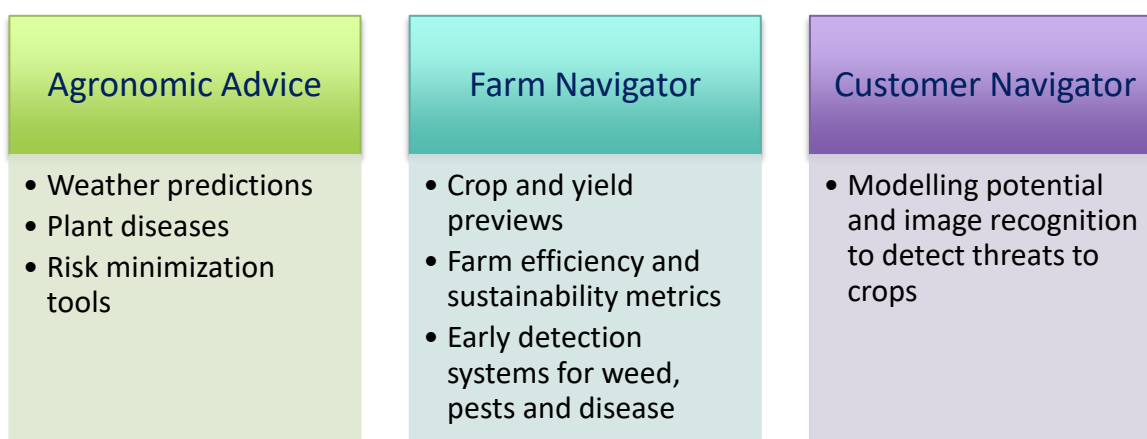
²⁶ BASF has embarked on two major data analytics projects: Compass™ and Maglis™ (Stroud 2018). Compass™ mobile farm data management system integrates crop management, GIS/GPS mapping, grain inventory management, and live agent support; to provide farmers with better farm management decisions (BASF 2018a). However, this data management system was 'transferred and assigned to Affinity Management Ltd.' on May 8th, 2018 (BASF 2018b).

²⁷ The Grow Smart™ with BASF programme states that farmers have limited chances to establish the right mix during each season in order to ensure the best possible yields are possible. There needs to be careful agronomic knowledge, careful planning and portfolio innovation to procure the best possible approach each year (BASF 2018e). The BASF Grow Smart™ University is their platform that provides the resources of agronomic knowledge and insights for the most productive and effective options the farmer should take (BASF 2018d). This website provides a range of free informative courses, webinars and videos on many different seed specifications, herbicides, insecticides, plant health, seed enhancement and agribusiness/market-place economic forecasting. Ultimately, BASF attempts to 'support farmers through several knowledge transfer initiatives' (Heldt 2018).

agricultural solutions for farmers (BASF 2017d). By combining these data with the company's agronomic knowledge and individual farmer data, it aims to provide solutions to 'help farmers use their resources more efficiently and sustainably' (Strip-Till Farmer 2017).

Maglis consists of three fundamental components: Agronomic Advice, Farm Navigator and Customer Navigator. Maglis Agronomic Advice provides farmers with local weather predictions, plant disease *in situ* detection, and recommendation of tools to minimise risk (BASF 2018c). Maglis Farm Navigator provides farmers with crop and yield previews, farm efficiency and sustainability metrics, and early detection systems for weed, pests and disease (BASF 2018c). Farm Navigator is used by the farmer to manage the agronomic activities of their field, by inputting when particular crops were sown, what kind of crops, so that the Navigator can provide outlines of how that crop should grow. Farm Navigator has large modelling potential and image recognition, which allows the farmer to see the growth cycle of crops and to detect potential threats to the crops. Maglis Customer Navigator is a support system for farming consultants who are working with farmers to find ideal agricultural planning solutions (BASF 2018c). The Customer Navigator is a Windows tablet application and is used by BASF advisers to engage with the farmers and to make recommendations about what products might help them. The software can be tailor-made for each farmer, by factoring in a multitude of data from their location, soil types, crops grown, weather predictions, and farm size.

Figure 4 – Components of BASF's Maglis™



BASF uses image-recognition software that receives images from the farmer, identifies particular crops, and recognises spots or abnormalities on the leaves for early disease detection. This software uses machine-learning techniques to analyse weather data to 'anticipate crop threats such as pests and disease' (Bunge 2017). The Interviewee 3 at BASF noted that the Maglis team are using a wide array of different Big Data and machine-learning tools, such as Hadoop Stack, SAP HANA, and cloud-based systems. The Maglis software also benefits from using data derived from other sources, such as field data from John Deere machinery and AI tools, such as PEAT image recognition. Interviewee 1 stated that BASF also invested in a Swiss start-up, ecoRobotix, through its venture capital branch. ecoRobotix are developing

'a robot that is spraying micro amounts of herbicides on wheats, which is a camera-assisted, self-driving, 130kg lightweight robot that moves automatically up and down in fields, and just treats the areas where weeds begin to grow' (Interviewee 1).

BASF have been providing technological solutions to farmers for over 100 years, and they view the data analytics service as the next logical step to help farmers achieve the best possible yield on their farms in a sustainable and effective manner (BASF 2016). They view the integration of Maglis as a way of reinforcing their goal of providing effective crop protection solutions. The Senior Vice President of BASF Crop Protection North America states that ‘farmers are collecting a lot of data’, and that ‘[t]hey want help in how to put that information to use’ (Paul Rea 2016). One of the aims of BASF is to provide farmers with answers far quicker than previously. Innovation Specialist, Neil Doherty, states that he was unable to get to a customer’s farm to provide guidance, but with remotely-accessible tools such as Maglis, help can be provided before incidents occur (Vogt 2016).

BASF have been providing technological solutions to farmers for over 100 years, and they view the data analytics service as the next logical step to help farmers.

One of the primary motivations for using SIS technology for BASF is the ability to make the farmer’s life easier, more productive, and to save costs (Interviewee 2). BASF wants to incorporate its sustainability paradigm through the use of Maglis technology. It allows farmers to identify their carbon footprint, their impact on biodiversity, and the environmental impact of their activities. Essentially, through Maglis BASF hopes to improve farming, not by increasing fertilizer use, but by more intelligent farming decisions and practices (Interviewee 1). There needs to be an investment in knowledge and the use of farm management software is one way that this can be optimized (Interviewee 1).

The Farm Navigator of Maglis is available on the web and can be used with most modern internet browsers and is available on Android and iOS tablet applications. However, there are no MAC versions available at present. Maglis is available free-of-charge and anyone with an internet connection can download the software (BASF 2016). Hence, it could potentially offer valuable services to farmers around the world, something too costly if done by sending trainers to these locations. However, it is hoped that the service can be charged for in the future.

3.3. Potential Technical Challenges of Using SIS for BASF

All three interviewees emphasized that Maglis is still in its very early stages of development. Their goal is to effectively communicate a wide range of recommendations to farmers. The sustainability component of the project was envisioned through a wish-list of what they would like the system to do and requirements that should be programmed into it. There is the hope that by mid-2019 users in Europe and Canada will be able to see:

‘the fully-fledged indicator systems for sustainability, presented in a nice way’ (Interviewee 2).

The Maglis service is supervised by human beings, carrying out regular analysis of the recommendations that it proposes. All three interviewees stated that they were aware that algorithms may be fallible. There is a wide array of disparities with variables that measure weather, soil and plant disease. These variants can cause a lot of difficulties for artificial intelligence algorithms (Bunge 2017). Despite the impressive data collection and analytic abilities of artificial intelligence, there may be ‘critical data points—such as crop yield or the ultimate impact of a dry spell— [which] only emerge once per year’ (Bunge 2017).

The image recognition software to detect plant disease has to be effectively trained on a very large and growing repository of images. BASF have created an algorithm that can be very helpful, if the data repository is sufficient. So far, they have hundreds of thousands of plant images in the repository. Furthermore, the system is only as effective as the datasets that it is being trained on. If the system is not trained on a particular dataset, i.e. a banana leaf, then the system will not be able to effectively identify what that image is. However, if you ask an agronomist, they will be able to tell you straight away that it is a banana leaf. Therefore, tools such as Maglis will not replace agronomists anytime soon, as there will always be exceptions where the farmer needs human expertise as a result of the lack of intelligence of machine-learning tools. The Interviewee 3 stated that when there are issues with their SIS, it is the result of data quality issues or lack of data, and not necessarily the algorithms. The algorithms work effectively with the training data that they are provided with, if there is poor or lacking data, then you get poor results.

The algorithms work effectively with the training data that they are provided with, if there is poor or lacking data, then you get poor results.

Also, there are natural variations from country-to-country and region-to-region, such as differences in pest management, climatic conditions, and crop types. BASF is aware that Maglis cannot establish a one-size-fits-all approach for their project and changes their algorithms for different regions. Another constraint lies in the actual labour power required to maintain many farm management systems, requiring a large department to work on it. Particularly, when it comes to ensuring the safety and security of the farmer's data.

Interviewee 1 said that recommendations to improve sustainability are dependent upon data availability and the ability to extract useful and meaningful information from this data. While there are interesting questions that would help their algorithms, farmers did not want to disclose certain pieces of information; for example:

'How much land do you dedicate to agri-environment schemes?' (Interviewee 2).

The focus of national sustainability discussions has also proved to make developing universal algorithms for all countries challenging because of their varying needs. For example, some countries like to talk about biodiversity, so it is incorporated into Maglis' algorithms, whereas in other countries different sustainability parameters take precedence.

3.4. Feedback from Stakeholders

The Maglis team received some negative feedback about particular aspects of Maglis and changed those features accordingly. One of the main challenges was creating simple and effective user interfaces, and external companies and consultants were employed to assist. Traditionally, BASF has been a b-to-b company²⁸, but Maglis differs in this approach because it can also be used by the end-user. Maglis pays close attention to user needs and incorporates feedback and input from farmers into the dashboard's functionality.

Feedback on Maglis was obtained through focus groups and farmer associations. Maglis was not a 'co-creation', according to Interviewee 1; but farmers were heavily involved in improving the tool. He stated that one of the main objectives of the Maglis project was to be able to make the

²⁸ Business to business company.

information provided to farmers accessible and understandable. Whether or not it would be successfully adopted and used depended on how effectively message were translated:

'We are nerds, we are geeks sitting here in an ivory tower and we like everyone to know all this stuff, but the real world is the world of the farmers, and we have to translate information in a way that farmers find this understandable and, to maybe [to] some extent, appealing' (Interviewee 2).

Because the platform is still in its infancy, the company is still working to identify how it has improved the lives of farmers and ways to improve it going forward.

'We start a pilot with a dedicated number of farmers, let's say 20, 50, 100. With these farmers, we have intense interaction. ... We repeat that for every country. You could say, "We have done the Farm Navigator. We've done it in the United Kingdom, so we can start it in Germany directly." No, we don't do that' (Interviewee 3).

BASF are aware of the different needs and effects of Maglis on stakeholders, so they need to carefully design it for each region. The Maglis team have worked with many different weather companies, dashboard design consultants, and advisory boards to develop Maglis. The SIS is sent for external review to ensure that it is fit for purpose and functions according to their intent.

Figure 5: Ethical issues identified from using SIS at BASF



4. BASF: Ethical Issues from SIS Technology

Throughout the three interviews conducted at BASF, and through desktop research conducted from the company's website and a number of other sources, certain ethical issues were highlighted as a result of using SIS technology in BASF. These issues largely reflect those found in the literature, as above, highlighting a great deal of correlation between academic understanding of the issues with those working in industry as below.

4.1. Accuracy of Data and Recommendations

One of the problems that BASF encountered initially was that not all farmers had data available to be evaluated because of poor record-keeping. An issue related to the plant recognition technology used to identify plant disease was the inability of some farmers to take clear pictures of the plants. If the image data is unclear, it is extremely challenging for the image recognition algorithms to determine what plant it is.

Data retrieved from third-party weather companies may not be accurate, and micro-climatic conditions may occur in certain fields that are not represented in the algorithms. So, for instance, if the weather data being put into the plant growth algorithm is inaccurate, there may be discrepancies with the growth predictions. The Interviewee 3 in BASF stated that the problem usually lies with the accuracy of the data being inputted into the system, rather than the algorithms, if there are issues or discrepancies with the system.

If the weather data retrieved from weather APIs is inaccurate, then it may lead to inaccurate growth projections in the Farm Navigator crop growth stage predictor. However, if these growth predictions are inaccurate because of misleading weather data, the farmer still has the ability to update the projections with what is happening in reality. For instance, if Maglis tells the farmer that his crop is at BBCH²⁹ stage 32, but it is at stage 36, they can reset and recalibrate the system. The Interviewee 3 at BASF mentioned that they are aware that the SIS will not be perfect every time and they have considered methods to counteract these errors.

Maglis gives prescriptive recommendations to the farmer, but if it gives inaccurate recommendations, who is held responsible or how is this problem resolved, is an important question for the project. When discussing potential issues with AI, Interviewee 1 gave the example of another project that BASF are working on, a robot that weeds and plants crops, their ecoRobotix project. In this example, Interviewee 1 stated that the worst thing that could happen is that crops are destroyed, but that because of the procedures set in place, error detection would either be straight away or within a day or two. Therefore,

‘damage that such a robot can do in one day is nearly negligible’ (Interviewee 1).

While most of these SIS are in their early development stage, and their impact and effect is quite small, it is still an important concern for the company and they stated that they are taking these factors on board.

4.2. Data Ownership and Intellectual Property

Issues surrounding data ownership and intellectual property are very important within the use and implementation of SIS technology and the data retrieved to make these processes work. Therefore, the types of data retrieved is an important factor to identify. After discussing this with the Interviewee 3 at BASF, he mentioned that there are a number of different types of personal data retrieved from the farmer:

‘we have his name, we have his email address, we have his phone number, mobile phone number if he gives it, we have his postal address if he gives it. The farmer is creating his farm, on Farm Navigator, at a certain location, so we have geo coordinates. The farmer is growing his fields, so we have – even – field locations’ (Interviewee 3).

²⁹ BBCH is a scale used to identify the phenological development stages of plants.

The Interviewee 3 also mentioned that it is a top priority for the company to securely protect this data from misuse, hacking, and the misappropriation for economic or marketing purposes. He stated that the company does not use the individual farmer's data to make comparisons between farms, and if this is done in the future, it would not be done without explicit informed consent from the farmers involved. The data are used for the benefit of the farmers, the improvement of the BASF algorithms, and the development of the BASF SIS technology.

Data are used for the benefit of the farmers, the improvement of the BASF algorithms, and the development of the BASF SIS technology.

All three interviewees made it explicit that the farmer owns their own data and they can move to a different farm management system supplier, with that data, if they choose to. During the interviews, it became clear that there needs to be a symbiotic mutually beneficial relationship between the farmer and the agribusiness in order to procure data to improve SIS:

'we are convinced that people are willing to share data if they have a benefit from that' (Interviewee 1).

It is aimed to help improve the farmer's yield, help sustain their business, and remove some of the costs from hiring agronomists. Using agronomists can be expensive, but the company is aware that their SIS would not replace the effectiveness of human input provided by agronomists.

4.3 Economic Issues and the Digital Divide

One of the key constraints in agriculture is the pressure being placed on farmers to produce more for less. There are great strains being placed on the farmer by large supermarket and food production companies to supply cheaper, more diverse, and quicker produce. Interviewee 1 noted that, the farmer does not have a great deal of bargaining power in this relationship. The hope of BASF is that tools like Maglis will enable the farmer to farm more effectively, thus alleviating some of the strains placed upon them. One key factor in the creation of Maglis was ensuring that it was affordable and easy to use for farmers, otherwise it would have been rejected in its implementation phase.

As noted earlier, Maglis is available free-of-charge and anyone with an internet connection can download the software (BASF 2016). One of the beneficial and essential components of Maglis is that it opens up the possibility of providing free advice to many poorer nations unable to afford agronomic advice, helping sustainable agricultural development in LMICs.

At the same time, if there were no economic incentive for the farmer, the software would be rejected. Therefore, there was a strong need to make the use of Maglis viable for the farmer. All three interviewees expressed the economic strains placed on farmers underpinned the success or failure of the SIS. If the system helps cope with the strain, it is more likely to be accepted.

4.4. Privacy and Security

The relationship between privacy and data security is a key concern for the company and it was clear that the two were very closely related, with the customer's privacy being ensured by strong security measures. The BASF Interviewee 3 noted that data security was a very high priority for the company and that they develop the latest methods to ensure their system is secure:

'Inside the system, passwords ... are encrypted. For storing the data, the general mechanisms of SQL³⁰ databases are used - also, for encrypting. The data is as secure as our system is, to prevent it being compromised by having an intruder there that can get his hands on the farmer's data' (Interviewee 3).

In order to ensure that this data security is maximized, the company hires third-party organisations to test their systems and to coordinate attacks to find issues or problems. The Maglis team are aware of issues surrounding reverse engineering to access the algorithms in Maglis, so they put great emphasis into securing all of their platforms. If BASF's servers are secure and Maglis is fully encrypted and secured, then there is little chance that farmers' data will be breached, according to the interviewees. The Maglis project works within BASF's code of ethics, so abides by BASF's use of customer data and other regulations. Interviewee 1 emphasized that they aim to promote transparency and legitimacy within Maglis,

'to make sure that what we defend in public is what we want to see also within the company' (Interviewee 1).

One of these goals is the strong emphasis within the company on sustainability, putting a dedicated focus into ensuring that sustainability goals and parameters are implemented into the SIS.

4.5. Environmental Protection

There were no customer requests to have a sustainability component put into Maglis, but the company viewed it as an important factor to integrate within the SIS. Interviewee 1 pointed out that when the usefulness of Maglis was explained to farmers, and that it can be used to comply with different regulatory procedures, it was more widely accepted. Interviewee 1 said that the Maglis project is aligning sustainability certification schemes within it in order to help farmers meet these certifications. The sustainability criteria were developed from the European PEF (Product Environmental Footprint) and the company's Life-cycle assessment (LCA) frameworks (European Commission 2018). However, Interviewee 1 is aware that countries will have different sustainability standards, so Maglis needs to account for these differences.

The Maglis project was launched in Canada and focused on providing advice within a Canadian context. BASF were aware that the algorithms used for Canadian farmers could not be universally used for farmers everywhere. Different algorithms are required because of the varying climatic conditions, crop types, and needs of farmers worldwide. Interviewee 1 stated that sustainability needs are local and require different sustainability parameters and there was a trial-and-error process in the beginning to fix bugs, as Maglis was a prototype. All three interviewees emphasized that this SIS was still in its early stages of development, but the company is working hard on resolving any issues that may arise. They are taking a fresh perspective in the industry by incorporating a sustainability component within their farm management system to anticipate future constraints placed on farmers, the environment, and society as a whole, in the future.

4.6. Employment

One element that emerged through the interviewees and less so through the literature research was employment. During the interviews, it became clear that farm management systems, like Maglis, would not replace the role of agronomists because the SIS technology is not advanced enough to account for a wide range of different variables and there are limitations within the technology itself.

³⁰ Structured Query Language.

The SIS technology is intended to *complement* the human expert, rather than replace them. Farmers may also prefer receiving advice from human beings, rather than receiving it from an impersonal SIS technology. Some farmers enjoy and benefit from the discussion and articulation of farming needs and prefer using a human advisor to using a software tool, like Maglis. Furthermore, SIS technology is fallible and very often farmers trust the advice of a human agronomist over artificially-intelligent created prescriptions. Farmers still do not fully trust the recommendations given by AI tools, such as Maglis, so still rely on the input from agronomists.

5. Conclusion

Despite the SIS applications in the agricultural sector, there are still many social and ethical issues during the integration and use of SIS technologies on farms. This case study demonstrated how SIS is being used in the agricultural sector and the relationship between farmer and ATPs. The three interviews offered perspectives into the real-world application of farm management systems and touched upon a number of practical, economic, and ethical issues in the use of SIS.

The ethical issues in the use of SIS in agriculture mapped onto those identified through the interviewees, with the exception of employment concerns. Issues of employment were not raised in the literature, despite being a widely discussed topic in the field of SIS. BASF state that their SIS will not hinder employment, as they are seen as compliments to agronomists, rather than replacing them. However, on the other hand, Maglis is offered free-of-charge, which reduces the costs farmers have to pay for agronomic consultancy, thus questioning the agronomist's purpose if the technology improves in the future.

The company also protects personal data stored about the farmer and acknowledges privacy concerns during the use and implementation of their SIS technology. In the case of Maglis, the farmer also retains ownership of their own data, which has been a huge concern in the literature.

While great efforts are being placed into the development of SIS, there are still restrictions and limitations to its effectiveness for implementation, as a result of the changing requirements for different countries. The Maglis team are aware of this and do not intend to roll out a universal SIS, stating that it needs to be tailored to specific needs of each region it is developed. The integration of stakeholders throughout the process was commendable, but going forward, the incorporation of stakeholder input prior to the use of this SIS may be valuable for the company.

The Maglis team are aware of the limitations of SIS and expressed the need to constantly develop their SIS modelling and improving their data quality. For instance, the plant image verification software will be trained more efficiently with larger image repositories, while the accuracy will be improved through training farmers to take better pictures. The company is also taking a very proactive approach towards sustainability agendas and issues, implementing sustainability parameters and advice to the farmer through Maglis.

5.1. Limitations

One of the main limitations of this report is that there were only three people interviewed from BASF. If it were possible to interview more people, from a wider diversity of roles on the project, it would have enriched the case study. Only one of the interviewees had hands-on experience with the technical side of the project (interviewee 2), the first interviewee's sole focus was on the

sustainability aspects of Maglis, whereas, the third interviewee had a more managerial role, and was a little more guarded about some of the answers that he gave about the project.

Maglis has only been effectively implemented in one country (Canada), and while it is being rolled out in a number of European countries, it is still in its very early stages of development. The Maglis team are still in the process of evaluating the effectiveness of SIS, so this proved to be a limiting factor in understanding its societal impact. Therefore, while we were able to discuss and address many of the issues that BASF face in their implementation of SIS, the case study could have been enriched if there were evaluations by the company to determine how it affected the Canadian farmers using it in a more empirical manner.

In addition, the case study was limited by only analysing one agribusiness. While efforts were made to incorporate more organisations into the case study, the larger companies using SIS either did not reply or pulled out of the case study with no explanation. Smaller agricultural companies were identified, but upon discussions with different members from their companies, it was discovered that their technologies are quite primitive, and certainly could not classify as SIS. Therefore, it was concluded that they would be invalid to participate in a case study on this topic.

5.2. Contribution to Knowledge

There has been very little written about BASF's role in the agricultural industry, as they are primarily a chemicals company, and even less about their use of SIS. This report provides valuable insights into their latest project Maglis and ethical considerations around its use. The analysis of Maglis contributes an empirical evaluation of agricultural SIS and how an agribusiness is responding to the ethical implementations of such technologies, such as concerns around privacy, security, accuracy of algorithms, accuracy of data, and employment.

Overall, the Maglis project is in its early stages of development, but there were still strong correlations between academic and practical issues regarding agricultural SIS, with many of the most pressing issues being identified in the interviews. While many of the ethical issues discussed have been analysed within academia in other applications of SIS, they have rarely been discussed in an agricultural context.

This report provides an effective literature review of the area and an original empirical evaluation of a large agribusiness using and implementing agricultural SIS. It provides a valuable contribution of knowledge to the discipline of Big Data/AI ethics, while also contributing to empirical research on the implementation of SIS technologies within the agricultural sector. It offers the areas of agricultural ethics, SIS theory, and the burgeoning topic of agricultural SIS, insights into ethical issues related to the use and implementation of SIS in the agricultural industry.

5.3. Implications of this Report

This report will offer insights to agribusinesses on the ethical issues found in the use and implementation of SIS. While only one ATP business was interviewed, this still accounts for 25% of those developing SIS (BASF, Bayer/Monsanto, DuPont Pioneer, and John Deere). Some issues that need to be addressed when integrating agricultural SIS are: how will it develop and what types of data will be required and will the farmer will have to pay for this service in the future. These issues needs to be addressed and made explicit to the end-user for its successful ethical implementation.

Another implication of this report is reinforcing the importance of identifying responsibility when SIS does not work as intended, or causes adverse effects as a result of its use. It was unclear if

there was an onus of responsibility on the company if negative effects occurred from using the technology. BASF should clarify in their terms of service and providing adequate informed consent to the farmer about this, and this should also be a prime concern for all agribusinesses implementing SIS on farms. This advice should apply to all agribusinesses working with SIS.

There has only been a handful of policy documents created to tackle issues relating to agricultural data and the integration of SIS technology in this domain. There are very few policy guidelines and frameworks for the ethical use of SIS in agriculture, so this case study offers policymakers some insights into how agribusinesses tackle these issues in practice, namely, who owns farm data – the farmer or the agribusiness? BASF instil that the farmer is the owner of the data, which is in distinction from companies like Monsanto and DuPont Pioneer.

5.4. Further Research

While this report offers an extensive literature review of the most pertinent ethical, social and legal issues of agricultural SIS, there may be additional matters that need to be evaluated in the future. This report evaluated a number of empirical studies conducted with farmers, the use of SIS technology, and their relationships with ATPs, but further empirical research in these areas would provide valuable insights and contributions to the domain. Furthermore, the field would also greatly benefit from additional case studies with the other three ATPs in this area (Bayer/Monsanto, DuPont Pioneer, and John Deere).

While this case study covered BASF's integration of SIS technology, the ethical issues pertinent within the other three ATPs may be quite different from those found in this report. It would be interesting to have these additional case studies available at some stage in the future to cross-examine the varying styles, implementations, and usages of SIS technology by different ATPs. Additional case studies are required to evaluate the differences between the use and implementation of agricultural SIS in North American (DuPont Pioneer, John Deere, and Monsanto), contrasted with European (BASF and Bayer) implementation of SIS would also offer some great insights into the field. It would also be highly interesting to see what agricultural ethicists and those working in lobbies opposing unethical actions of large agribusinesses, would say about the development of agricultural data analytics.

6. References

- Antle, John, Susan Capalbo, and Laurie Houston, "Using Big Data to Evaluate Agro-Environmental Policies", *Choices* Vol. 30, Issue 3, Autumn 2015, pp. 1-8.
- BASF, "2018 BASF Grower Solution", 2018a, retrieved June 27th, 2018. <https://industries.BASF.com/assets/north-america/us/en/Agriculture/Crop%20Protection/Growers%20Advantages/WI.pdf>
- , "BASF and Proagrica Sign Agreement to Offer Interface for Farm Management Systems", 2017a, retrieved June 28th, 2018. <https://www.BASF.com/en/company/news-and-media/news-releases/2017/08/p-17-292.html>
- , "BASF and the European Space Agency to Develop Digital Services for Farmers", 2017b, retrieved June 27th, 2018. <https://www.BASF.com/en/company/news-and-media/news-releases/2017/02/p-17-127.html>

- , "BASF Launches Maglis, a New Online Platform to Help Farmers Improve Crop Management", 2016, retrieved June 28th, 2018. <https://www.BASF.com/en/company/news-and-media/news-releases/2016/03/p-16-140.html>
- , "BASF Signs Agreement to Acquire Significant Parts of Bayer's Seed and Non-Selective Herbicide Businesses", 2017c, retrieved June 28th, 2018. <https://www.BASF.com/en/company/news-and-media/news-releases/2017/10/p-17-336.html>
- , "BASF to Strengthen Digital Farming Offer with Acquisition of Zedx Inc.", 2017d, retrieved June 28th, 2018. <https://www.BASF.com/en/company/news-and-media/news-releases/2017/04/p-17-192.html>
- , "An Important Announcement Regarding Compass Grower", 2018b, retrieved June 27th, 2018. <https://agro.BASF.ca/compassgroweradvanced/#>
- , "Maglis® – Today's Digital Solutions for the Agriculture of Tomorrow", 2018c, retrieved June 26th, 2018. <https://agriculture.BASF.com/en/Crop-Protection/Decision-Support-Maglis.html>
- , "Welcome to BASF Grow Smart University", 2018, retrieved June 27th 2018d. <https://BASFlms.publicishawkeye.com/login/index.php>
- , "With About 40 Chances in a Lifetime, It Pays to Grow Smart", 2018e, retrieved June 28th, 2018. <https://agriculture.BASF.com/us/en/Crop-Protection.html>
- Bedford, Laurie, "BASF Set to Acquire Zedx", *Successful Farming*, 2017, retrieved June 27th, 2018. <https://www.agriculture.com/news/technology/BASF-set-to-acquire-zedx>
- Bennett, John, "Agricultural Big Data: Utilisation to Discover the Unknown and Instigate Practice Change." *Farm Policy Journal* Vol. 12, Issue 1, Autumn 2015, pp. 43-50.
- Bronson, Kelly, and Irena Knezevic, "Big Data in Food and Agriculture." *Big Data & Society* Vol. 3, Issue 1, January – June 2016, pp. 1-5.
- Bunge, Jacob, "Agricultural Giants Teach Computers to Farm", 2017. *The Wall Street Journal* retrieved June 28th 2018. <https://www.wsj.com/articles/leaf-recognition-technology-agriculture-digs-into-artificial-intelligence-1505300400>
- , "Dupont Sees \$500 Million in Annual Revenue from Farm-Data Services", *The Wall Street Journal*, 2014, retrieved 27th June 2018. <https://www.wsj.com/articles/dupont-sees-500-million-in-annual-revenue-from-farm-data-services-1393515676>
- Byarugaba Agaba, G, et al., "Big Data and Positive Social Change in the Developing World: A White Paper for Practitioners and Researchers", Rockefeller Foundation Bellagio Centre Conference, 2014. <https://www.rockefellerfoundation.org/report/big-data-and-positive-social-change-in-the-developing-world/>
- Carbonell, Isabelle, "The Ethics of Big Data in Big Agriculture", *Internet Policy Review*, Vol. 5, Issue 1, March 2016, pp. 1-13.
- Carolan, Michael, "Publicising Food: Big Data, Precision Agriculture, and Co-Experimental Techniques

- of Addition", *Sociologia Ruralis* Vol. 57, Issue 2, December 2017, pp. 135-54.
- Castle, Mike, Bradley D Lubben, and Joe Luck, "Precision Agriculture Usage and Big Agriculture Data." *Cornhusker Economics* Vol. 725, May 2015, pp. 1-4.
- Coble, Keith H, Ashok K. Mishra, Shannon Ferrell and Terry Griffin, "Big Data in Agriculture: A Challenge for the Future", *Applied Economic Perspectives and Policy* Vol. 40, Issue 1, May 2018, pp. 79-96.
- Darr, Matt, "Big Data—the Catalyst for a Transformation to Digital Agriculture", Proceedings of the 26th Annual Integrated Crop Management Conference, 2014.
- European Commission, "The Environmental Footprint Pilots", European Commission [website], 2018, available here: http://ec.europa.eu/environment/eusd/smgp/ef_pilots.htm
- Ferris, Jody L, "Data Privacy and Protection in the Agriculture Industry: Is Federal Regulation Necessary." *Minn. J. Sci. & Tech*, Vol. 18, Issue 1, 2017, pp. 309-342.
- Interviewee 1, "Interview", at BASF Agricultural Centre Limburgerhof, 22/08/2018.
- Interviewee 2, "Interview", at BASF Agricultural Centre Limburgerhof, 22/08/2018.
- Interviewee 3, "Interview", at BASF Agricultural Centre Limburgerhof, 22/08/2018.
- Heldt, Markus, "BASF, Crop Protection Involves a Response to Changes." *Agriculture Internationale*, 2018. June 28th, 2018. <http://www.agriculture-internationale.com/en/english/farming/BASF-der-pflanzenschutzsektor-muss-sich-dem-wandel-anpassen.html>
- Hirafuji, Masayuki, *A Strategy to Create Agricultural Big Data*, 2014 Annual SRII Global Conference (SRII), 2014, IEEE.
- Infosys, "BASF and Infosys Strengthen Partnership to Develop New Digital Services for Smarter Farming", 2018. June 28th, 2018. <https://www.infosys.com/newsroom/features/Pages/digital-services-smarter-farming.aspx>
- Kamilaris, Andreas, Andreas Kartakoullis, and Francesc X Prenafeta-Boldú, "A Review on the Practice of Big Data Analysis in Agriculture." *Computers and Electronics in Agriculture* Vol. 143, October 2017, pp. 23-37.
- Kosior, Katarzyna, "Agricultural Education and Extension in the Age of Big Data", *European Seminar on Extension and Education*, 2017.
- Kshetri, Nir, "The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns", *Big Data & Society* Vol. 1, Issue 2, 2014.
- Kumari, S Vinila, P Bargavi, and U Subhashini. "Role of Big Data Analytics in Agriculture." *IJCSME*, 2016.
- Lokers, Rob, Rob Knapen, Sander Janssen, Yke van Randen, Jacques Jansen, "Analysis of Big Data Technologies for Use in Agro-Environmental Science", *Environmental Modelling & Software*, Vol. 84, 2-16, pp. 494-504.

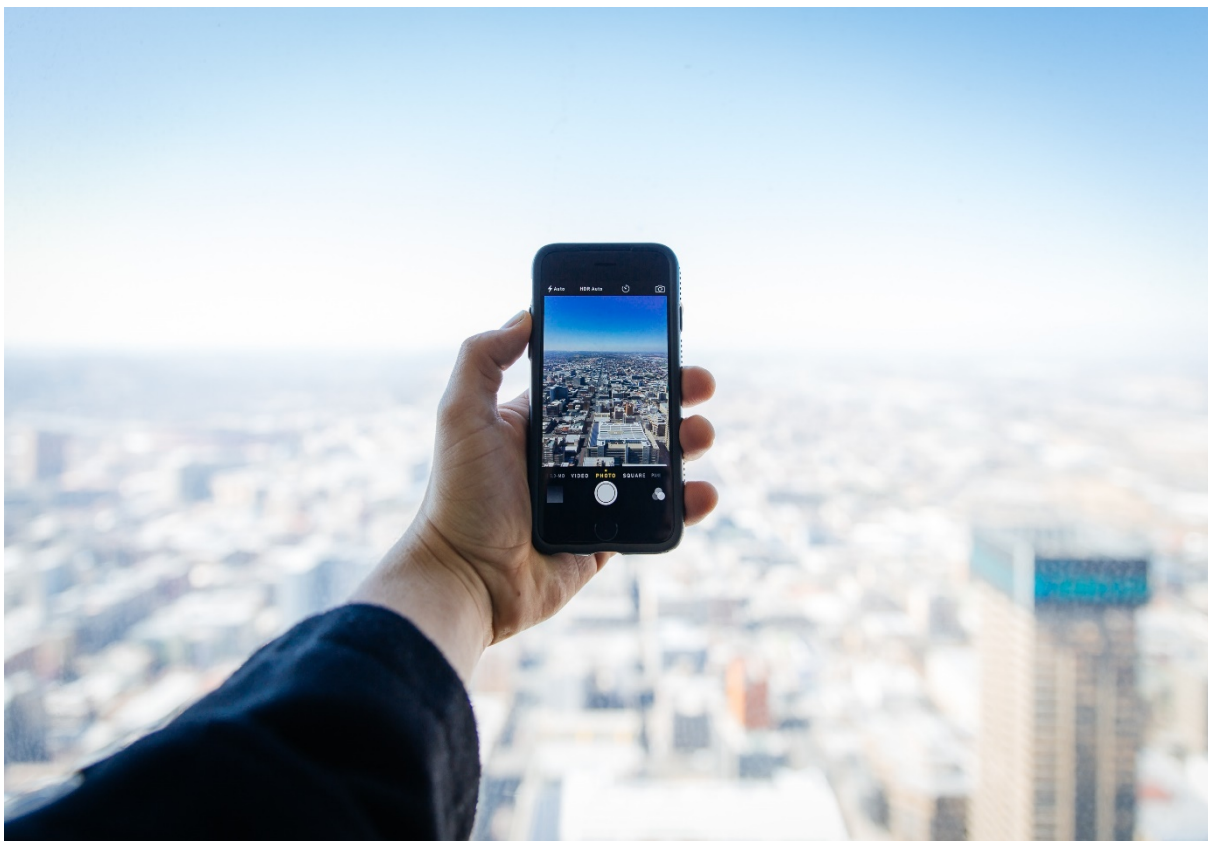
- Micheni, Elyjoy Muthoni, "Diffusion of Big Data and Analytics in Developing Countries", *The International Journal of Engineering and Science* Vol. 4, Issue 8, 2015, pp. 44-50.
- Mintert, James, David Widmar, Michael Langemeier, Michael Boehlje, and Bruce Erickson, *The Challenges of Precision Agriculture: Is Big Data the Answer*. Southern Agricultural Economics Association Annual Meeting, San Antonio, Texas. 2016.
- Morota, Gota, Ricardo V. Ventura, Fabyano F. Silva, Masanori Koyama, and Samodha C. Fernando, "Machine Learning and Data Mining Advance Predictive Big Data Analysis in Precision Animal Agriculture", *Journal of Animal Science*, 2018, pp. 1540-1550.
- O'Grady, Michael J, and Gregory MP O'Hare, "Modelling the Smart Farm", *Information Processing in Agriculture*, Vol. 4, 2017, pp. 179-187.
- Panicker, Remya, *Adoption of Big Data Technology for the Development of Developing Countries*. Proceedings of National Conference on New Horizons in IT-NCNHIT, 2013.
- Popa, Cosmin, "Adoption of Artificial Intelligence in Agriculture." *Bulletin of University of Agricultural Sciences and Veterinary Medicine Cluj-Napoca. Agriculture*, Vol. 68, Issue 1, 2011, pp. 284-293.
- Poppe, Krijn, Sjaak Wolfert, and Cor Verdouw, *How Ict Is Changing the Nature of the Farm: A Research Agenda on the Economics of Big Data*. 11th European IFSA Symposium, Farming Systems Facing Global Challenges: Capacities and Strategies, Proceedings, Berlin, Germany, 1-4 April 2014. 2014.
- Rea, Paul, "Crop Protection Company Rolls out New Ag Data Tool." Ed. Vogt, Willie. Farm Industry News website: Farm Industry News, 2016.
- Ribarics, Pal, "Big Data and Its Impact on Agriculture." *Ecocycles* Vol. 2, Issue 1, 2016, pp. 33-34.
- Rosenheim, Jay A, and Claudio Gratton, "Ecoinformatics (Big Data) for Agricultural Entomology: Pitfalls, Progress, and Promise." *Annual review of entomology*, Volume 62, 2017, pp. 399-417.
- Schönfeld, Max v, Reinhard Heil, and Laura Bittner, "Big Data on a Farm—Smart Farming", *Big Data in Context*. Springer, 2018. pp. 109-20.
- Sonka, Steve, and Yu-Tien Cheng, "Big Data in Farming: Why Matters!" *farmdoc daily*, Vol. 5, Issue 211, November 2015.
- Strip-Till Farmer, "BASF Acquires Digital Ag Intelligence Company, Zedx", *Strip-Till Farmer*, 2017, retrieved June 27th, 2018. <https://www.striptillfarmer.com/articles/2349-BASF-acquires-digital-ag-intelligence-company-zedx>
- Stroud, Christina, "BASF Strengthens Digital Farming Portfolio with Zedx Acquisition", 2018, retrieved June 27th, 2018. <https://agro.BASF.ca/BASF/agprocan/newsroom.nsf/readWE/NR-OAIO-ALXPJL?openDocument>
- Sykuta, Michael E. "Big Data in Agriculture: Property Rights, Privacy and Competition in Ag Data

- Services", *The International Food and Agribusiness Management Review*, Vol. 19, Issue A, June 2016, pp. 57-74.
- . "The Fallacy of "Competition" in Agriculture", in Harvey S. James, Jr. (ed.), *The Ethics and Economics of Agri-food Competition*, Springer, 2013. pp. 55-73.
- Talavera, Jesús Martín, Luis Eduardo Tobón, Jairo Alejandro Gómez, María Alejandra Culman, Juan Manuel Aranda, Diana Teresa Parra, Luis Alfredo Quiroz, Adolfo Hoyos, and Luis Ernesto Garreta, "Review of IoT Applications in Agro-Industrial and Environmental Fields", *Computers and Electronics in Agriculture*, Vol. 142, September 2017, pp. 283-97.
- Taylor, Linnet, "Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World", in Linnet Taylor B. van der Sloot, and L. Floridi, *Group Privacy: The Challenges of New Data Technologies*, Springer, 2017. pp. 13-36.
- The World Bank, "Employment in Agriculture", The World Bank [website], 2018, available here: <https://data.worldbank.org/indicator/SL.AGR.EMPL.ZS>
- Taylor, Linnet, and Dennis Broeders, "In the Name of Development: Power, Profit and the Datafication of the Global South", *Geoforum*, Vol. 64, 2015, pp. 229-37.
- Tzounis, Antonis, Nikolaos Katsoulas, and Thomas Bartzanas, "Internet of Things in Agriculture, Recent Advances and Future Challenges", *Biosystems Engineering*, Vol. 164, September 2017, pp. 31-48.
- UN Global Pulse, "Big Data for Development: Challenges & Opportunities", *Naciones Unidas, Nueva York*, mayo, 2012.
- USDA NASS. *2012 Census of Agriculture Highlights: Farm Economics*, 2014.
- Vogt, Willie. "Crop Protection Company Rolls out New Ag Data Tool", *Farm Industry News*, 2016, retrieved June 28th 2018. <http://www.farmindustrynews.com/precision-farming/crop-protection-company-rolls-out-new-ag-data-tool>.
- Wolfert, Sjaak, et al. "Big Data in Smart Farming—a Review", *Agricultural Systems* Vol. 153, 2017, pp. 69-80.
- Wolfert, Sjaak, Claus Aage Gron Sorensen, and Daan Goense, *A Future Internet Collaboration Platform for Safe and Healthy Food from Farm to Fork*. Global Conference (SRII), 2014 Annual SRII, 2014. IEEE.
- Zhang, Haoran, Xuyang Wei, Tengfei Zou, Zhongliang Li, and Guocai Yang, *Agriculture Big Data: Research Status, Challenges and Countermeasures*, International Conference on Computer and Computing Technologies in Agriculture, 2014, Springer.
- ZedX Inc. "About Zedx, Part of BASF Group", 2017a, retrieved June 27th 2018. <https://www.zedxinc.com/company/>
- . "Building Tomorrow's Agricultural Business Intelligence Today", 2017b, retrieved June 28th 2018. <https://www.zedxinc.com/>

CS04 – Sustainable Development



Ethics of Using Smart City AI and Big Data: The Case of Four Large European Cities



**This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641**



Document Control

Deliverable	Deliverable 1: Case Studies
WP/Task Related	WP1: Representation and Visualisation
Delivery Date	31/1/2019
Dissemination Level	Public
Lead Partner	Mark Ryan
Contributors	Mark Ryan University of Twente Anya Gregory European Business Summit
Reviewers	
Abstract	
Key Words	

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes
0.1	14/11/2018	Mark Ryan and Anya Gregory		
0.2	21/11/2018	Anya Gregory		Revision and conclusion
0.3	23/01/2019	Mark Ryan and Anya Gregory		

Contents

Executive Summary	115
Smart Cities and SIS: An Ethical Analysis	116
1. The Use of SIS Technology in Smart Cities	117
2. Ethical Issues of Using SIS in Smart Cities	118
2.1. Conflicts of Interests and Bias.....	118
2.2. Economic Pressure	119
2.3. Inequalities.....	119
3.4. Privacy	120
3. A Case Study: Four Organisations Using Smart City SIS	122
3.1. Description of the Organisation(s) and Individual(s)	122
3.1.1. Amsterdam CTO	123
3.1.2. Copenhagen Solutions (City Data Exchange)	123
3.1.3. Deutsche Telekom (MySMARTLife).....	124
3.1.4. Helsinki Municipality	125
Table 1.1 – Interview details with four organisations	125
3.2. Description of SIS Technologies Being Used	125
3.2.1. Amsterdam CTO	125
3.2.2. Copenhagen Solutions (City Data Exchange)	126
3.2.3. Deutsche Telekom (MySMARTLife).....	127
3.2.4. Helsinki Municipality	128
3.3. SIS Technologies Effectiveness During Use.....	128
3.3.1. Amsterdam CTO	128
3.3.2. Copenhagen Solutions (City Data Exchange)	128
3.3.3. Deutsche Telekom (MySMARTLife).....	129
3.3.4. Helsinki Municipality	129
3.4. Stakeholder Engagement	130
3.4.1. Amsterdam CTO	130
3.4.2. Copenhagen Solutions (City Data Exchange)	130
3.4.3. Deutsche Telekom (MySMARTLife).....	130
3.4.4. Helsinki Municipality	131
4. Ethical Analysis of Smart Cities Using SIS	131
4.1. Accuracy of SIS and Bias.....	132

4.2. Availability and Accuracy of Data.....	132
4.3. Economics and Inequalities.....	133
4.4. Privacy and Data Ownership	134
4.5. Transparency and Trust	135
5. Conclusion	136
5.1. Limitations.....	136
5.2. Contribution to Knowledge.....	137
5.3. Implications of this Report.....	138
5.4. Further Research.....	138
6. References	139

Executive Summary

By 2030, the population living in cities will increase by an additional 1.5 billion people, placing a great strain on resources, infrastructure, jobs and healthcare (UN 2018). It has become clear that to combat this change, a number of creative approaches need to be put in place to ensure the sustainable growth of cities - one such approach being the 'smart city' (UN 2018). Due to the relative infancy of smart cities, and the diversity of approaches and implementations of smart information systems (**Big Data and AI**), many of the ethical challenges are still being defined.

One of the reasons behind this challenge is a result of the varying **smart information systems (SIS)** being used in different urban contexts. This case study hopes to unpack some of these ethical challenges by looking at four different applications of SIS being deployed in large European cities: a citizens' complaints AI (**Amsterdam**), a parking permit chat-bot (**Helsinki**), a platform for data exchange (**Copenhagen**), and a project with an open-source algorithm (**Hamburg**). Upon first glance these technologies seem very disparate, but they all factor into the equation of what goes into making a smart city, 'smart'.

What quickly became clear was that smart cities are in their infancy, which meant that **availability and accuracy of data** remains an issue in a large majority of the cases. In terms of the **accuracy of recommendations** – due to the early stages of smart city implementation, many projects remain wary of expanding the usage of SIS, due to potentially unforeseen issues and are proceeding cautiously.

Data was once previously espoused as a 'cure-all' in the urban planning and business worlds has been debunked and has taken on a new role as a less-offensive and potentially helpful tool for citizens and planners alike to regain control and access of information within their respective cities. **Consent, transparency and data ownership** featured as prominent ethical considerations in all cases, especially the focus on citizens regaining control over their own data. It remained a point of contention to whom the data would belong – with an overall consensus that data should remain the property of the citizen or municipality and not necessarily that of private companies.

Collaboration is at the heart of a successful Smart City. Many of the projects utilised a collaborative **public-private** model to facilitate both the business development side and the **citizen-engagement** sides of the Smart City. With differing degrees of success in the individual projects, this remained an important feature that experts believe continue to develop in tandem with smart city projects. A bottom-up approach is clearly the most effective way to ensure that a smart city works and is used by citizens.

'At the end of the day (you want to ensure) they use it rather than you have a dull city...which is full of technology, but no one wants to live there and it's maybe not useable because the people don't understand it' (Interviewee 3, MySmartLife)

Overall, this case study offers valuable insights into the development of smart cities in a European context, the use and implementation of SIS in urban environments, and what kind of ethical issues are evaluated in the literature and how they contrast and diverge from those faced by professionals in practice. It is hoped that this case study will offer practitioners, policymakers, smart city organisations, and private ICT companies, some interesting observations about ethically-responsible approaches towards SIS implantation in smart city projects.

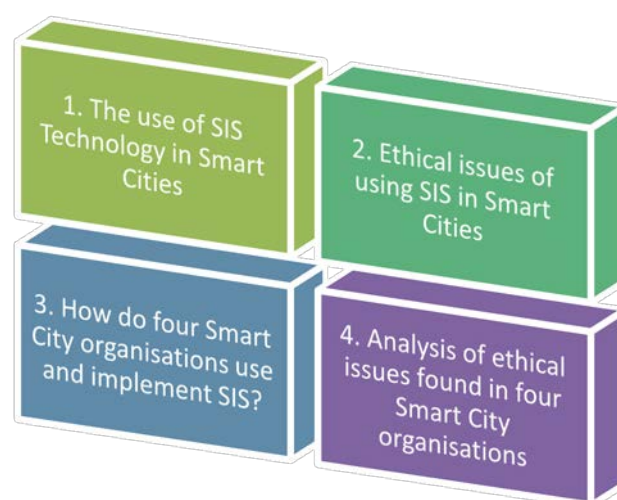
Smart Cities and SIS: An Ethical Analysis

In 2015, the UN General Assembly established 17 key sustainable development goals to aim towards by the year 2030. These range from eliminating poverty, to providing universal education, gender equality, and climate action. Goal 11 strives towards achieving sustainable cities and communities because the population living in cities will increase by an additional 1.5 billion people by 2030 (totalling 5 billion), which is set to place a strain on resources, infrastructure, jobs, and healthcare (United Nations 2018). The UN has established that we need to implement creative approaches to handle these changes. There is a need to reduce ecological harm, pollution, and injustice on the one hand; while increasing safe and affordable housing, improving infrastructure, and providing safe cities for people to live in (United Nations 2018). As a result, a number of approaches have been proposed to ensure sustainable cities, such as the ‘smart city’ concept.

The smart city concept dates back to 2008 and ‘is marked by real-time, interactive, and intelligent systems’ (Li, Cao, and Yao 2015, p. 2). A smart city ‘is one whose economy and governance is driven by innovation, creativity and entrepreneurship, enacted by smart people’ (Kitchin 2014, p. 2). There have been many different definitions of the smart city, but it is typically grounded on a drive towards technological innovation to improve the lives of city-dwellers. Emerging technologies, such as smart information systems (AI and Big Data), offer us the potential to create more sustainable cities (Kitchin 2013; Kitchin 2014). However, it is important that this is done in an ethical manner, which will be the focus of this case study.

A smart city is typically a city grounded on a drive towards technological innovation to improve the lives of city-dwellers.

Throughout this case study, the primary research question will be: Which ethical issues arise in the use of SIS when striving towards smarter cities and how can these ethical issues be addressed? Answering this question will be achieved by reviewing some of the most pertinent issues within the literature and by conducting interviews with four organisations involved in the implementation of smart city technologies (Amsterdam CTO, Copenhagen Solution’s City Data Exchange, MySMARTLife project in Hamburg, and Helsinki municipality). The aim of this case study is to identify ethical issues in the literature and if they correspond to those faced by organisations in practice. The report has four main sections:



Sections 1 and 2 focus on theoretical work and the literature within the field, while sections 3 and 4 assess the organisations we interviewed between September and November 2018.

1. The Use of SIS Technology in Smart Cities

The definition of a smart city is often contested. IBM first coined the term in 2008 as referring to the integration of 'smart' technology within a city, either a pre-existing city or a newly created smart city, such as: Masdar near Abu Dhabi (developed by General Electric), Paredes in Portugal (developed by Microsoft), Dongtan in the Yangtze Delta (developed by Arup), and Songdo in South Korea (developed by Cisco) (Batty et al. 2012).

One of the binding components within smart city definitions is that they place a strong emphasis on the adaptation and integration of technology within cities, revolutionising how they function in practice. However, while not all definitions of a smart city contain strict adherence to the widespread endorsement and incorporation of technological development, technology usually plays a strong role in *most* smart city definitions:

The term *Smart City* is a broad term that refers to the *smart* management of the cities socio-economic and environmental capital through the use of Information and Communication Technologies. These technological solutions are said to be *smart* as they provide ways to enable social, cultural and urban development, improving social and political capacities and/or efficiency (Vázquez-Salceda et al. 2014, p. 15-7).

The majority of academics, policymakers and individuals working on smart cities, discuss the fundamental role that technology will play in urban areas, particularly their widespread implementation and use of the Internet of Things (IoT), Artificial Intelligence, (AI), Big Data and Information and Communication Technology (ICT) infrastructure (Nigon et al. 2016). In an analysis of smart city literature, out of 125 different reports, 91% discussed how cutting-edge technologies and ICT were key factors; with AI being the most widely discussed technology (Rjab and Mellouli 2018). In smart city definitions, technology is applied to a wide number of applications: health, waste management, air quality monitoring, noise monitoring, transportation management, energy consumption, resident living environment, security, parking, lighting and infrastructure (Guo et al. 2018; Zanella et al. 2017, p. 23). Overall, the use of technology in smart cities can be categorised into six domains: economy, people, governance, mobility, environment and living (Albino, Berardi, and Dangelico 2015; Kitchin 2015b; Voda and Radu 2018, p. 111).

Figure 1: Use of technology in smart cities



Many claim that technology is an overriding 'meta-factor' that is intertwined and engrained in all of the domains of a smart city due to the use of a wide array of different technologies to retrieve vast amounts of data from a city and its citizens (Chourabi et al. 2012). Some of the technologies used

to retrieve data are digital cameras, sensors, transponders³¹, GPS³², kiosks, meters, personal devices, appliances, social networks, and machine-readable objects (Kitchin 2013, Kitchin 2016b). These technologies are used to monitor activity in the city by way of traffic lights, traffic speeds and traffic flows, criminal activity, movement of pedestrians, number plates, media access control (MAC) addresses, faces and gaits, transport meter readings, energy usage, and environmental pollution (Kitchin 2015a, p. 4).

Retrieving this data from such an array of sources requires input from a wide array of stakeholders. These stakeholders include utility companies, transport providers, mobile phone operators, travel and accommodation websites, social media sites, crowdsourcing and citizen science, governmental bodies, financial institutions and retail chains, private surveillance and security firms, emergency services, and entertainment systems (Kitchin 2016b, p. 2).

While the range of stakeholders providing data is vast, the number of companies using and implementing this data in smart city projects is restricted to a few big ICT companies namely General Electric, IBM, Cisco Systems, Siemens AG, Microsoft, Oracle, SAP, Intel, Arup, Alcatel, Hitachi, Fujitsu, and NEC (Albino, Berardi, and Dangelico 2015; Batty et al. 2012; Hollands 2015; Kitchin, Lauriault, and McArdle 2015; Sholla, Naaz, and Chishti 2017).

These companies are proposing ambitious plans for cities adopting their SIS technology, but it is important to identify the challenges and issues that may arise when implementing these technologies to ensure that the applications are ethically sound.

2. Ethical Issues of Using SIS in Smart Cities

Discussing and questioning ethical issues in the application of Smart City SIS technology remains an underdeveloped area of research. While many academics have analysed the *conceptual* idea of a smart city, few of them concentrate on the use and implementation of SIS technology within the smart city paradigm. Even the journal *Smart Cities* carried few relevant articles on SIS *implementation*.

To overcome this lack of immediate academic information, keyword searches were conducted, using multiple different variations for relevant articles for this case study, through a number of bibliographical databases: Google Scholar, ScienceDirect, Web of Science and Scopus. This provided a wide diversity of articles for this report. Their analysis showed the ethical issues fall broadly into four categories, which are presented below.

2.1. Conflicts of Interests and Bias

Major projects can be built bottom-up or top-down. Responsible innovation (Owen et al 2013) favours the inclusion of all relevant stakeholders in the development of major innovative projects such as smart cities. However, it is claimed in the literature that smart city ideologies are laden with neoliberal agendas whilst being packaged as socially just, inclusionary and sustainable projects (Kitchin 2014; Kitchin 2015b). This indicates that a top-down approach is prevalent. Smart cities, SIS and algorithmic governance have the potential to prioritise vested interests and values, benefiting corporations and state bodies, rather than citizens (Cardullo and Kitchin 2017; Kitchin 2016a).

Many smart city initiatives are devised by SIS technology corporations and city governments, disregarding civic participation and civic input (Foth 2017; Hollands 2015). As a result of the huge push towards technological advancements, this may lead to an overemphasis on the 'the smart', much to the detriment of 'the city' (Galdon-Clavell 2013, p. 718). Smart city initiatives may place a greater

³¹ A device for receiving a radio signal.

³² Global Positioning System (GPS), a satellite-based radio-navigation system.

emphasis on technical fixes, instead of implementing political and social solutions to try to tackle urban issues (Kitchin 2015a, p. 9).

There are also many corporations using the smart city template as a test-bed for new technologies to sell their products (Kitchin 2015a, p. 9). However, due to the top-down nature of their invested interests, there is the concern that the involvement of third-party companies will have a detrimental effect on the organisation, decision-making and management of cities. Corporations are providing advice, guidance and implementing technologies within cities, and this may not be done impartially or in the best interests of the city (Kitchin et al. 2017). For example, IBM Smart City Index initiates different ranking methods to measure smart cities' development. This Index demonstrates a conflict of interests since companies like IBM are currently selling SIS to cities while also ranking competing cities based on their index.

The technology drive behind the smart city philosophy may be seen as the *best, or only* solution, to create sustainable urban environments. However, it does not consider the diversity and range of city habitats (Kitchin 2016a), which require equally diverse solutions. Advocating for the widespread adoption of smart city SIS may lead to the view of cities as homogenously interchangeable (O'Grady and O'Hare 2012, p. 1581). Smart city initiatives treat cities as though they are devoid of historical, spatial and cultural significance; 'treating cities as if they are all alike in terms of their political economy, culture, and governance' (Kitchin 2015a, p. 9). Even 'new' smart cities are distinctly different from pre-existing smart cities, further reinforcing the discrepancy of a one-size-fits-all approach (Shelton, Zook, and Wiig 2015). As such, smart city SIS may lead to the wiping out of cities' individuality and diversity (Foth 2017).

Due to the invested interests and general top-down approach to Smart City, some authors request that smart cities need to incorporate citizens into the design, use and implementation of SIS to ensure they are meeting the needs of the community (Grey, Dyer, and Gleeson 2017, p. 48).

2.2. Economic Pressure

Most cities are far from reaching the desired benefits outlined in smart city agendas because they are still in the early stages of development (Kitchin 2016b). Therefore, it is presumptuous to imply that all cities adopting the smart city ideology, guided by SIS, will become successful. At the same time, monetary benefits are increasingly linked to efforts to become smart. Smart cities are being heralded as a pioneering and benchmarking initiative to strive towards. Cities will be ranked in terms of the 'smartness' (i.e. SIS development) and in turn, will receive increases or decreases in their national investment, foreign direct investment, and tourist trade (Kitchin, Lauriault, and McArdle 2015, p. 25). Therefore, the use of smart city SIS technologies may 'augment the cities competitiveness' (Voda and Radu 2018, p. 110); while others argue that 'AI is what makes a smart city 'smart'' (Srivastava, Bisht, and Narayan 2017). The use of SIS may allow cities to develop or else lose out on investment, development, and progress (Batty et al. 2012).

2.3. Inequalities

While there is a widespread promotion of SIS, there is concern that the technology may replace humans in many areas of the smart city (Munoz and Naqvi 2017, p. 7). Many people fear that SIS will replace customer service, driving, and factory jobs within the coming decade. In a recent Eurobarometer survey, 74% of people believed that there will be greater job losses than job creation as a result of robots and AI (Capgemini Consulting 2017). There are also a number of practical requisites to accommodate an AI smart city: physical infrastructure modifications; intellectual infrastructure; informational infrastructure; governance and regulatory; and socio-economic (Munoz and Naqvi 2017). Smart cities need an intellectual infrastructure to deploy SIS, becoming hubs for technological innovation and advancements, which may subsequently lead to a 'brain-drain' in rural

areas. The most educated and prosperous citizens will be located in cities, which could have a dramatic effect on the education, prosperity, and growth of rural areas.

Despite the potential negative effects of smart cities, if they are used inappropriately or there are vested interests at stake, they also offer the possibility of great benefits to cities. However, there is still the potential that SIS will create digital divides and inequalities, despite these benefits. For example, *wealthier areas within cities* may develop quicker than poorer areas. SIS is largely aimed at middle-to-upper class individuals who want a more technologically-savvy city. They are often more concerned with efficient services and amenities, rather than social inequalities within their city (Kohli 2014). Therefore, SIS may disadvantage poorer citizens *within* a city, because city officials are appealing to middle-to-upper class interests. Furthermore, poorer citizens may not be able to afford to use these technologies, even if they were available in their areas (Glasmeier and Christopherson 2015, p. 10).

With the introduction and development of smart city SIS, inequalities, power asymmetries and the wealth gap could become exacerbated. This could happen on several levels, from a global standpoint with the wealthier countries developing at a much quicker rate, to cities within a country or even to the local neighbourhoods becoming drastically different due to an increase in technology in one neighbourhood. Smart city projects may also further reinforce current power symmetries and inequalities *between* cities, rather than tackling them at their root (Kitchin 2015a, p. 9). Rich cities will be able to implement and use SIS technologies, increasing productivity by up to 40%, while poorer cities get left behind (Munoz and Naqvi 2017, p. 4). This will cause a divergence between cities that can afford to implement SIS and those that cannot. While SIS may bring positive change for cities, they may also exacerbate inequalities with a 'digital divide' between cities (Chourabi et al. 2012, p. 2291).



Cameras Image, Pexels free stock photos

3.4. Privacy

There are many different concerns that arise when discussing privacy in the context of Smart cities, such as the use of technologies that track movement, technologies that scan bodies, and those that record and recognise audio. Due to these concerns, in order for citizens to accept SIS within public space of the city, privacy must be ensured (Bartoli et al. 2011).

Body scanners, a technology that is largely being used in airports, could also be used in a number of different urban contexts. Body scanners are inherently intrusive; they scan individuals'

bodies, revealing private aspects of oneself, such as medical conditions and appliances, body piercings, and prosthetics (Finn, Wright, and Friedewald 2013, pp. 11-12). Currently, most body scanners are controlled by humans; but the start-up Evolv, which is funded by Bill Gates, is testing the use of AI-checking body scanners in cities (Harris 2016).

Protection of one's property and physical space and overall privacy is very important to individuals (Kitchin 2016c, p. 5). With the use of these intrusive technologies, the protection of individual's privacy may become more difficult. SIS technology has recently proliferated and is now found in our vehicles, homes, and belongings. These technologies have become crucial for easy of public spaces, amenities, and services with apps being used for transit and services such as Google Maps being used regularly. With these daily SIS in mind, it becomes even more important that the data gathered in these 'private' spaces does not fall into the wrong hands to be used in a malicious way.

A respect of privacy is crucial for citizens to accept SIS in their public space.

Since Smart cities are based on the collection and use of data through SIS technologies, safeguarding the data is crucial for the maintenance of the goal of a Smart City to benefit citizens. The benefits of using SIS to collect data within the Smart City context can be enormous – but the question remains as to who has access to this data and how to protect this data from a security breach. For example, audio detection, voice recognition, electronic communication monitoring, recording and processing software can all be used to help safeguard the security of citizens in the case of a public issue (violence, theft etc.) The SIS technology has advanced rapidly, and Google has recently developed AI that can single out one voice from a crowd of people (Tung 2018). Similarly, DeepMind has been developing AI that can successfully lip-read what individuals are saying (Condliffe 2016). SIS such as these may safeguard smart city security, but they may also be used to infringe upon ordinary citizens' communication privacy.

Individuals may also want to ensure their privacy is protected in relation to their movement, purchases, transactions, and queries (Kitchin 2016c, p. 5). For example, individuals making queries about smart parking or smart bus services may have this data used to determine the patterns and habits of the user (Martínez-Ballesté, Pérez-Martínez, and Solanas 2013). Again, this kind of data can improve the accuracy and effectiveness of a service or in the wrong hands promote malicious intent or be used for commercial purposes (such as targeted advertising).

After evaluation the ethical issues in the literature on the use of SIS in smart cities, we can identify a wide number of concerns that need to be addressed. However, it is unclear if these issues are being identified and addressed in practice on smart city projects. The following sections will evaluate four organisations working on smart city projects to determine if the ethical issues found in the literature correlate with those in real-life examples. We chose these four projects because they cover a wide array of areas within smart city SIS implementation, such as: how do private companies see their involvement in these projects (MySMARTLife interviewee), ethical issues around the exchange of Big Data between private and public organisations (City Data Exchange), how to implement AI for the benefit of the public in an ethical manner (Helsinki municipality), and how can municipalities develop their own SIS and team to integrate it (Amsterdam). The case study also uses four advanced smart city projects to demonstrate how North European cities are implementing SIS in practice (Amsterdam, Helsinki, Copenhagen, and Hamburg).

3. A Case Study: Four Organisations Using Smart City SIS

This section will focus on four organisations using SIS technology within city contexts. The organisations that collaborated with us provide a good diversity of viewpoints about the use and implementation of SIS technology in Europe since they are working in different cities with different technological projects and platforms.

When we undertook our background research about smart cities in Europe, we found that a lot of the smaller cities and the organisations involved in these projects were approaching them theoretically, or else the integration of smart city technology was in its infancy stage, making it difficult to find appropriate projects to analyse. We wanted to interview organisations advanced in their development of smart city SIS technology, covering four major European cities (Amsterdam, Copenhagen, Hamburg, and Helsinki). Three of the organisations (Netherlands, Denmark, Finland) involved in our case study are within the top four rankings of the most advanced digital economies in the EU (European Commission 2018).

We conducted interviews with four individuals between September - November 2018. Before conducting these interviews, we compiled background research on the organisations and their use of smart city technologies. This information was retrieved from the organisations' website, policy documents, and newspaper articles on the projects. During the interviews, we discussed their involvement with SIS and if ethical issues became apparent in the process. We analysed the interviews using a qualitative analysis software tool (NVIVO) in order to understand, define, and assess the content of the interviews. In a two-day [SHERPA](#) consortium workshop, the group evaluated interviews from 11 case studies and established a wide range of different topics, nodes, and themes from our interviews. This allowed us to effectively analyse the initial interviews from this smart city case study. Where necessary, we completed follow-up interviews to elucidate areas that were not clear in the initial interview.

3.1. Description of the Organisation(s) and Individual(s)

The following section will detail the organisations, projects and technologies used to assist in giving context to the analysis.



Amsterdam, photo, Pexels free stock photos

3.1.1. Amsterdam CTO

Amsterdam municipality has attempted to take a proactive approach to the development of its city, initiating a number of 'smart', technological and innovative solutions for current problems. Amsterdam has been pioneering European smart city development, assisting over 80 smart city projects since 2009; collaborating with 250 tech stakeholders; receiving Europe's Capital of Innovation prize in 2016; and being ranked 3rd in the Global Innovation Index 2017 (Brokaw 2016; Macpherson 2017).

Amsterdam municipality aims to improve the city through six thematic areas: digital city; energy; mobility; circular city; government & education; and citizens & living (Roose 2015). One of the driving forces behind it is the Chief Technology Office (CTO), developing Big Data and AI projects to promote sustainability and citizen happiness. There are over fifty people employed in the CTO (Daalder 2018), and they work with Amsterdam municipality to encourage innovation through: 'e-health, circular economy, smart mobility, sharing economy, cooperation with start-ups and innovative procurement' (Amsterdam Smart City 2018a).

Interviewee 1 works for the CTO Innovation Team of the city of Amsterdam in an advisory/strategy role on how to incorporate AI to prepare the municipality for the future. She also works for the Public Tech programme,

'In which we investigate new technologies and what their impact is on society, on the organisation, on our citizens' (Interviewee 1).



Copenhagen, photo: Doris Schroeder

3.1.2. Copenhagen Solutions (City Data Exchange)

The City Data Exchange was a collaborative project between three organisations: The Municipality of Copenhagen, the Council Region of Copenhagen, and Hitachi. The project began in 2013 from public investment and ran for 5 years (concluding in 2017). The purpose of the project was to examine the possibilities of 'creating a marketplace for the exchange of data between public and private organizations', and was seen as a way to test the 'readiness of the market to deliver new data-sharing solutions' (Municipality of Copenhagen and Capital Region 2018, p. 2).

The technical platform is an IT solution for displaying, selling and purchasing data. It includes the ability to upload datasets for sale, to identify relevant datasets based on a series of criteria, to see metadata, to sample data and to purchase datasets. The data portal is 'open' and all data is

aggregated and made anonymous. The interviewee, Interviewee 2, is responsible for the technical and data challenges at Copenhagen Solutions Lab and works for Copenhagen Municipality's open data platform, and for the city's share in the national open data platform, opendata.dk (Copenhagen Solutions Lab 2018).

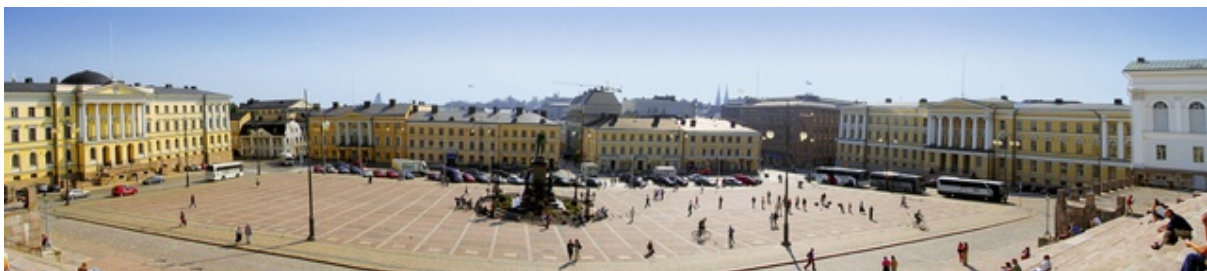
3.1.3. Deutsche Telekom (MySMARTLife)

Deutsche Telekom is a leading German telecommunications company, with 168 million mobile customers, 28 million fixed-network lines and 19 million broadband lines worldwide (Deutsche Telekom 2018). It is present in over 50 countries, with 216,000 employees and it generated € 74.9 billion in 2017. The company also offers business-to-business services, with their own division T-Systems accounting for over 38,000 employees in 20 countries worldwide. T-Systems is involved in transforming cloud-based services, integrating innovative projects for business, through data analytics, IoT, and machine-learning techniques (Deutsche Telekom 2018). Deutsche Telekom is also implementing many of these practices in smart city projects throughout Europe, and our interviewee 3 is involved in many of these.

Interviewee 3 participates in various smart city working groups like Digital Gipfel, Bitkom and is co-chair of the DIN Smart City Standards Forum. He is involved in several European projects like rethink (www.rethink-project.eu) developing concepts for a decentralized communications architecture and a Smart City Application concept together with the City of München (Munich) and the EU H2020 Lighthouse Project "Grow Smarter". In 2012, he worked on the project "XIFI," the second part of the EU project series around "FIWARE". Since 2016 he has been the project lead for Deutsche Telekom at the EU Lighthouse project MySMARTLife (www.mysmartlife.eu), which was the focus of the interview.

MySMARTLife began in 2016 and is a Smart City pilot project that includes three 'lighthouse cities': Hamburg, Helsinki and Nantes. MySMARTLife is funded under the EU's Horizon 2020 research and innovation programme with 27 partners from 6 countries, *'collaborating to make sustainable cities with smart people and a smart economy a reality'* (Interviewee 3).

There are three zones of intervention where the project MySMARTLife will be implementing the project in the borough of Bergedorf in Hamburg, which we focused on during the interview. The 'integrated strategy' comprises Zone 1, where more than 1,400 residential units will be built with smart controls and connection to a low-energy district heating and smart adaptive lighting for bicycle routes. Zone 2, 'the retrofitting area' – where Smart Heating Islands will be the main feature alongside a lamppost retrofit to be more environmentally efficient. Zone 3 is the mobility intervention using electric buses, e-cars, e-bikes and e-bus charging stations. This also includes a multi-modal mobility concept and innovative approaches like car-sharing e-community and parcel delivery system.



Helsinki, Photo: Sava Marinkovic, free images

3.1.4. Helsinki Municipality

Helsinki comprises 26 municipalities with 1.6 million inhabitants, generating over a third of Finland's Gross Domestic Product (GDP). Helsinki's location, harsh climates, and an ageing population means that the municipality is keen on innovative and pioneering ideas to advance and improve citizen welfare. A number of key technological and transformative projects to improve citizens' lives have been developed, increasing sustainability while improving business and job creation. One of the notable examples of this was the creation of Helsinki Smart Region, which aims to promote smart activities within Helsinki, by incorporating 'business, cities, public sector, research, education centres, start-ups and the citizen', to create 'sustainable mobility services, a healthy corporate environment, excellent living conditions' (Helsinki Smart Region 2018a).

Finland holds the fourth largest GDP share of expenditure on R&D (UNESCO Institute for Statistics 2018); the country is one of the leading digital hubs and is ranked first for country's global impact for global innovation; it is second in best global network readiness and fourth in terms of digital performance in the EU; while Helsinki is the fourth best start-up ecosystem in Europe (Helsinki Smart Region 2018b). One of the key areas of investment and development is AI and Big Data analytics. We interviewed Interviewee 4, who is the Chief Digital Officer within the Helsinki municipality. Interviewee 4 is involved in multiple visualisation projects integrating new technologies and works on projects analysing Big Data and AI, looking at how algorithms make decisions and are used within society, specifically their use in a Helsinki context.

Table 1.1 – Interview details with four organisations

Description	Organisation 1	Organisation 2	Organisation 3	Organisation 4
Organisation	Amsterdam CTO	City Data Exchange	Deutsche Telekom	Helsinki Municipality
City	Amsterdam	Copenhagen	Hamburg	Helsinki
Sector	Public	Public	Private	Public
Name	Interviewee 1	Interviewee 2	Interviewee 3	Interviewee 4
Length	48 minutes	45 minutes plus 30 min follow-up	45 minutes plus 30 min follow-up	49 minutes

3.2. Description of SIS Technologies Being Used

This section will detail and describe which technologies by each company/project and the reasons for its implementation.

3.2.1. Amsterdam CTO

Interviewee 1, our interviewee, is involved in many projects, such as Signals (or Signalen in Dutch), which is a system for citizens to report their complaints or feedback about what is happening in their neighbourhood. For example, if a citizen sees a broken streetlight, garbage has not been collected, or there is a rat problem, they have the opportunity to report these incidences through an app or on the website. The innovation team use NLP (Natural Language Processing) to determine what citizens are saying in order to be able to help them quickly and effectively. Citizens can log their complaint anonymously or provide their name, telephone number, and additional information. These

complaints are then sent to the relevant departments, i.e. the police department or the waste management department. The SIS technology also identifies if multiple complaints come from the same person, or if multiple people make complaints about the same issue, in which case it is prioritised.

Amsterdam CTO also has a chat-bot for the 'I Amsterdam' website called Goochem, which tells people about upcoming events in Amsterdam. The chat-bot is in Dutch, but there is the aim to develop it in English. Another project that Interviewee 1 is working on is determining asset management within the city through the use of panoramic images and image recognition AI. This SIS is used to evaluate panoramic images to determine if specific areas have traffic signs and if these match the records that the municipality have. It is in its early stages of development, but it is hoped that this technology will be used for a wide range of asset management in the city. They also have an open data website called City Data³³, which has a wide range of different datasets available. It is an open platform which encourages citizen engagement with these datasets.

3.2.2. Copenhagen Solutions (City Data Exchange)

The primary motivation in the City Data Exchange was to create an innovative platform for the exchange of data. The goal for this exchange was to improve the quality of life for citizens and the business environment of the region, through a partnership with Hitachi. Hitachi provided a cloud-based technology platform to exchange data between data brokers and companies requiring access to this data. Interviewee 2, our interviewee, explained that the platform was able to handle different kinds of data and was agnostic³⁴ in terms of input and output. Pricing was set by the data suppliers or data publishers on a per download basis. Interviewee 2 indicated that it was not a particularly technologically savvy algorithm that was used, stating it as:

'input- presentation – output' (Interviewee 2).

He noted that it was an uncomplicated systems delivery platform. According to Interviewee 2, the project had no ethical issues because it was a purely technical platform. He saw the project as a technical solution to a technical problem.

'From an ethics point of view, I feel that both the initial layout of the project and also the actual delivery was pretty straightforward and has no ethical impacts' (Interviewee 2).

³³ <https://data.amsterdam.nl/#?mpb=topografie&mpz=11&mpv=52.3731081:4.8932945&pgn=home>

³⁴ In the context of IT technology, 'agnostic' means something (e.g. a software, hardware, business process) that can be operated on various systems.



Image, MySMARTLife graphic from <https://www.mysmartlife.eu/>

3.2.3. Deutsche Telekom (MySMARTLife)

Our interviewees' work (Interviewee 3) centres on the 'digital transformation' aspects of a city and MySMARTLife focuses on designing new ways to shape the digital ecosystem of the city. According to the project plan, there are two phases of the project: the 'doing phase' and the 'monitoring phase', which will run until 2019. Part of the pilot project is a retrofit³⁵ of mobility interventions, these will be completed by the end of 2019. Overall, MySMARTLife has three main levels of activities: "Inclusive Cities", "Smart People" and "Smart Economy". "Inclusive Cities" refers to offering a high quality of life to residents, "Smart People" refers to the citizen engagement in the city's development. Smart Economy refers to the economic level aimed at increasing employment,

'attracting talents and providing goods and services according to the actual requirements' (Interviewee 3).

The project planned technological solutions in connection with refurbishing buildings, utilising renewable technologies, clean transport and ICT solutions (MySMARTLife 2018a). Interviewee 3 describes the technology as agnostic, with regards to their cloud system. Regarding the used ICT system, based on OGC³⁶ standard already used in Hamburg and the DT Smart City Lab approach using oneM2M, he described their approach as cloud agnostic & interoperable, avoiding a vendor lock-in often feared by cities and communities. A standardized ICT back-end (open urban platform) guarantees interoperability and sustainability in terms of availability.

'You can do it, you can program it yourself' (Interviewee 3).

There are two different methods of data collection being used, the first includes open data which is already being collected by the city of Hamburg through things such as electric mobility charging points. There is the aim that new data collected from 'objects' (i.e. smart street lights) will be integrated with existing data so that cities such as Hamburg can use this data to successfully govern their city. The project is doing this by ensuring that this data is usable. The purpose of the

³⁵ The addition of new technologies to older systems.

³⁶ Open Geospatial Consortium is an international organisation that tries to ensure quality open standards for the geospatial community.

project is to integrate new data collected by way of street lights and mobility into existing data. The key motivations for this are to ensure sustainability in the energy sector, successfully implementing mobility goals, and improving traffic flow in cities. Interviewee 3 has worked on ensuring the platform's interoperability as an open urban standardised platform.

3.2.4. Helsinki Municipality

In Spring 2018, a team of 15 – 20 people developed an agenda to utilize machine-learning techniques for better customer experience and citizen engagement. The Helsinki municipality realised that this is one way that they can digitalise the city and transform some of their currently existing services. One way that they are doing this is through the use of AI chat-bots that respond directly to citizens' requests online. This service was developed initially to help the citizens of Helsinki to acquire parking permits but is hoped to be used and integrated for a wide array of different services in the future.

The chat-bot was built using IBM Watson technology because that is the web portal that the city runs on, so it was the obvious choice for the municipality. Interviewee 4, our interviewee, said that they were open to input from organisations specializing in the chat-bot development, such as Accenture and Boost AI in Norway. The chat-bot uses SIS technology and learns through supervised learning methods, but it is still limited to type-recognition. While there are ambitions to develop the chat-bot to detect voice recognition, they aim to improve text-recognition before developing voice recognition.

3.3. SIS Technologies Effectiveness During Use

3.3.1. Amsterdam CTO

Interviewee 1 mentioned that Amsterdam is starting an algorithmic auditing project with KPMG in November 2018 to look at the effectiveness of the algorithms that they use to determine if they are fit-for-purpose or if they need to change any aspects of them. The purpose of this auditing is to determine whether their SIS technologies are working effectively and to demonstrate the municipality's emphasis on transparency and to receive a critical third-party analysis of their projects.

'So, the decisions that are made by the algorithm, do they represent the algorithm? And is it implemented in a way that is correct? Do we have control over it? Like, do we monitor the decision that it makes?' (Interviewee 1).

Interviewee 1 mentioned that there are interaction and collaboration between computer scientists creating algorithms and those working in the policy/legal division of the municipality to ensure that their algorithms abide by legislation. However, she was unsure if they continued collaboration with the policy/legal division after this period.

3.3.2. Copenhagen Solutions (City Data Exchange)

One of the expected impacts of the City Data Exchange project was to improve innovation in the region by creating a platform to facilitate data exchange. However, during the project, several problems became evident. The first was that each individual company had very different needs and expectations of the actual information derived from the data. The data requested was very specific and very expensive to deliver to a single customer. Throughout the project, the developers attempted to find ways to bundle the demands for data, but it was difficult to find a one-size-fits-all

solution. Unfortunately, there were quite a number of transactions - alluding to the failure of the platform as an intended marketplace. The main reason for this was due to the

'organisations having to both find the publishers or the suppliers and the customers' (Interviewee 2).

This was a major impediment to the effectiveness of the platform. The platform was espoused as being able to handle a lot of different kinds of data, but sometimes there were tensions between the demands of the customers and the intended use of the platform:

'They (the companies using the platform) needed a specific supplier for their specific problem' (Interviewee 2).

The data that was most interesting for the buyers (people movement patterns) was one of the most difficult to acquire. The idea of a general platform of data exchange was ineffective and on reflection Interviewee 2 noted that if revisited the platform would only be a specific platform based on specific-use cases rather than a general platform. He noted that a more effective approach should be based on general traits from the specific-use cases:

'Public innovation should be built on experience and not expectations' (Interviewee 2).

3.3.3. Deutsche Telekom (MySMARTLife)

Due to the project's ongoing nature, the technology appears to be working as intended. Interviewee 3 maintains that the technology is relatively simple and at this stage there was nothing to report back in terms of effectiveness. This is something that could be revisited at a later stage once the project has culminated, if the opportunity arose.



*Image from
<https://www.mysmartlife.eu/>*

3.3.4. Helsinki Municipality

Interviewee 4 raised the point that they are aware that they need to identify ways to integrate these new technologies and platforms within their currently existing platforms, which may not always be straightforward. There is a need for better understanding of SIS technologies and how they function so that they can be incorporated into feasible and effective ways. Furthermore, the team that is using and integrating these technologies need to be aware of how they may potentially affect the relationship and dynamic of the team using them and for those that will interact with them. The use of AI is different from traditional ICT because

'it's more dynamic, rather than static' (Interviewee 4).

However, he is aware of the limitations of the technology that they are using, that there are better chat-bots available on the market, so they are constantly looking for better options, solutions, and technologies to implement, within their budget constraints. He also noted that the chat-bot that they were integrating had difficulties that a lot of other chat-bots do not face, namely, trying to understand the Finnish language. While text-recognition technology has been developed for the Finnish language, it may not be as advanced as the technology available to recognize English.

3.4. Stakeholder Engagement

3.4.1. Amsterdam CTO

Interviewee 1 stated that the aim of a digital city, and understanding how AI technologies impact a city, were very important for the municipality. One way of understanding this is by receiving citizen feedback, which Amsterdam retrieves through a 'Demo Thursday', which allowed the municipality to discuss their SIS projects with the public:

'So, everyone that comes along is able to say something or ask stuff or try to think of better ways to work with the whole plan' (Interviewee 1).

Amsterdam Innovation Team places a great deal of importance on SIS that may have an effect on people and Interviewee 1 acknowledged that if they want to have

'an algorithm or if we want to apply machine learning for a really serious cause with really important decisions made by a machine then it should be so well investigated upfront because you can't make any mistakes. Because you have all these people here to take care of and you don't want to do something bad' (Interviewee 1).

She stated that most of the rules that civil servants follow is common sense and are already captured in the civil servant oath. Amsterdam municipality AI experts are aware of these and factor these principles into their projects. However, she is aware that sometimes there are 'grey areas', where it becomes a little unclear about the best course of action to take.

3.4.2. Copenhagen Solutions (City Data Exchange)

With the City Data Exchange, the stakeholders who were involved were largely the city of Copenhagen in collaboration with Hitachi (the platform provider). In contrast to the other projects, the main goal of the project was not citizen engagement but rather that of bettering business in the region.

Image: <https://www.mysmartlife.eu/network>

3.4.3. Deutsche Telekom (MySMARTLife)

Interviewee 3 stated that one of the grant requisites was citizen engagement, which was a big part of the project (MySMARTLife 2018b). Each city has a plan for how to discuss things with the people and for how to integrate them into the project. While he aims to incorporate citizen engagement within the projects, citizens were not engaged prior to the implementation of the project. He identified this as a 'difficulty' and the 'weak spot of the project' because professionals



'start from a technology perspective and they talk to the people rather than the other way around' (Interviewee 3).

He maintained that the majority of people will not understand the intricacies of the project and SIS technology, despite having very high expectations of the project:

'90 per cent of the people won't understand you anymore because you are so deep in the subject' (Interviewee 3).

He emphasizes that in order to include people in the discussion the topics need to be simplified. Some of the methods Hamburg is using to achieve this are the project office, the website, posters and a questionnaire. Citizen engagement is viewed by Interviewee 3 as integral to the project because

'at the end of the day they use it rather than you have a dull city...which is full of technology, but no one wants to live there and it's maybe not useable because the people don't understand it' (Interviewee 3).

In order to do this, they aimed to support cities by integrating a range of different stakeholders in the projects. There are also industrial stakeholders in each pilot project. For Hamburg, the industrial stakeholders are VW and Deutsche Telekom. There are also regional partners, two universities and city companies as well as the city itself.

3.4.4. Helsinki Municipality

Helsinki municipality developed their chat-bots because they viewed them as good user interfaces for many of the services they provide, a tool that could increase access to information between the municipality and the citizen. Using chat-bots there are a number of ways that citizens can engage with the municipality about voicing their opinions about the use of SIS. For example, there are apps and the municipality website where they can lodge complaints or concerns about any issues they want to raise, and these requests are then sent to the relevant department or division.

So, if they have any issues with the chat-bot, then those working on it will receive the concerns and feedback. In addition to accommodating citizens' concerns about SIS, there is a need to have fully qualified individuals working in the municipality on SIS. Interviewee 4 indicated that the municipality is creating different relationships with specialists developing AI in the city; for example, it is being taught in Helsinki University, which has over 20 AI specialists in a range of different fields.

4. Ethical Analysis of Smart Cities Using SIS

As a result of the four interviews conducted with the organisations discussed in the previous section, a few important overlapping ethical issues became prevalent when implementing SIS technology in practice:



The issues discussed in the interviews broadly reflect the same issues that are found in the smart city literature on the topic. There is a great deal of correlation and understanding of the most pressing ethical issues within the application of SIS technology in smart cities. While some projects had a greater concern for certain topics (i.e. Copenhagen and Helsinki had economic concerns), all shared an understanding of the importance of other ethical issues, such as privacy and data ownership. Overall, the organisations all wanted to achieve the best possible results in their respective projects and to use SIS to provide accurate recommendations and added benefit to society, as a result.

4.1. Accuracy of SIS and Bias

Determining the accuracy of information and bias are both crucial components to the case study's validity. Interviewee 4 said that the chat-bot is still in its early stages of implementation for car parking permits and they are aware that there will be teething issues in the process. They hope that within the next half year they will be able to develop scenarios and protocols for when the bot does not work as intended. So far, the SIS technology appears to be working quite effectively in the demo stages and the hope is that the chat-bot will be able to understand the intent of the customer to provide them with sufficient information about their requests. Once it has been implemented, there is a process to determine whether it is working effectively, and the customer has the ability to give feedback about their experience.

Interviewee 4 also indicated that there were ways to effectively train their algorithms on useful data, such as calls logged from customers to the department, but was aware that this may invade privacy and violate the General Data Protection Regulation (GDPR). Therefore, they will look into the possibility of indicating to customers that their data would be used in this way and receive informed consent to do so. He indicated that all of the data would be anonymised and aggregated, so there would be no privacy violation of sensitive or personal information. He stated that there is a strong focus on having sufficient training for those working with machine-learning to ensure that they are aware of how it functions and to identify possible issues as a result of using it. Interviewee 4 mentioned that the disadvantages or harmful effects of using the chat-bot are minimal in comparison to other applications of SIS. He stated that the worst that could happen is that the chat-bot does not work effectively, then the customer can just use the traditional way of getting the parking permit. It would be a minimal inconvenience, but he is aware that if it is used for other services, it may create greater issues.

This is very interesting because Interviewee 1 raised a similar concern about Amsterdam's implementation of SIS. She states that they are still in the developmental stage and their system is being used in situations that will have minimal negative impacts on the lives of Amsterdam citizens, such as with the example of the panoramic images project. It is not really a big problem if the SIS is ineffective, as the only real issue is that they will not have accurate information about the traffic lights in the city to compare with their own data on traffic lights. However, one way that the department is combating potential issues with their SIS is by conducting external third-party algorithmic auditing from KPMG, in order to ensure they are working according to intent. This is to ensure that they work how they are supposed to and provide benefit to the people of Amsterdam.

4.2. Availability and Accuracy of Data

Interviewee 2 indicated that there were very few problems with the technical parts of the project but delivering results was not straightforward. The Copenhagen City Data Exchange was originally conceived as a general platform based on the idea that data is interchangeable, but in practice, the specificity of data-usage undermined this original idea:

'Talking about it as a general resource is obscuring the ability to provide value' (Interviewee 2).

It was difficult to collect data from businesses because they were concerned it would affect their competitiveness. Interviewee 2 identified that the availability of data in itself was not sufficient for the creation of the marketplace due to the specificity of the needs from individual clients. He mentioned that if their platform had succeeded, it might have run into other issues, such as the data supplier with a valuable dataset may wanting some kind of control over how it is used.

Interviewee 3 noted that data availability is a fundamental requisite for the success of Smart City Projects, but in practice, this can be difficult. While Interviewee 4 also stated that data is very valuable nowadays and if algorithms have good training data they can work more optimally. He indicated that algorithms depend on the accuracy of data they are trained on, so there is a constant process of developing better procedures for acquiring and testing this data to ensure that it is fit-for-purpose.

Interviewee 4 hoped that the municipality will be able to retrieve and use their own training data for their algorithms, rather than relying on third-party vendors for this. While he was aware that they need to use vendors in a wide array of contexts for the successful integration of SIS technology, they do not want to become locked in by those organisations. The municipality wants to avoid dependence on third-party companies and is trying to create its own training data. This was a very interesting insight because Interviewee 2 also highlighted the fact that it was often difficult to retrieve data from private companies because they viewed the Copenhagen City Data Exchange platform as “parasitic” and of no benefit to them. Unless there was an identifiable benefit for the companies, they did not want to take part in the projects. However, Interviewee 3, who works for one of these private companies (Deutsche Telekom), indicated that they actually want to give control to the city. The city should

‘own and reign over the data, not a company’ (Interviewee 3).

Interviewee 3 stated that city officials should work with private partners for the responsible collection of data. It is important that cities work together with private companies to form an ‘agreement’ for the purpose of data collection. Overall, this interaction between public-private was an interesting area of discussion with the interviewees and it appeared that the tensions were often underpinned by economic interests.

4.3. Economics and Inequalities

Interviewee 3 stated that smart cities are about collaboration between corporations and municipalities and not simply the sale of services according to a standard business model. He also mentioned that there are many issues to overcome, such as bureaucratic hurdles or negotiations with investors showing the difficulty of economics versus sustainability since renewable energy solutions are often not priced competitively - this complicates and slows down the projects he is involved in. In the City Data Exchange project, the city of Copenhagen and the council region of Copenhagen initially invested the funding into the project and hoped that Hitachi would develop the project further. In terms of Hitachi’s benefit from the project, Interviewee 2 mentioned that

‘they won an offer and got some seed capital to start up the organisation and the project’ (Interviewee 2).

According to Interviewee 2, Hitachi gained smart city acknowledgement and credit as a result. He stated that there was a tension between public and private entities within the project and indicated that public entities focus on providing value to citizens whereas this may have been a hindrance in the economic development of this project. One of the problems with Hitachi’s involvement was the limitation of public funding as

‘it forced them to continue the project beyond what they would normally do’ (Interviewee 2).

If the outcome were a Hitachi product, it probably would have been terminated earlier, as they would have prioritised their invested interest. It would have been deemed as too costly and loss-making to continue. This private sector response of ensuring profit can be contrasted with how public sector organisations may respond to the implementation of SIS. For example, Interviewee 4 indicated that the Helsinki municipality has an obligation to ensure job security for its staff,

regardless of SIS efficiency. He stated that because it is the public sector, their jobs are protected, and if anything, the chat-bots are designed to take the strain off them and aid in their positions:

'they are training the software robot to handle more and more tasks, and I understand that it's been very welcome; there are a lot of mundane, routine tasks that now can be given to the software robot, and it needs to be trained' (Interviewee 4).

The use of SIS technology within Helsinki municipality would not cause job losses, but rather reduce the workload of employees in the public sector. There is the aim to have more services automated:

'instead of people answering questions, a machine can answer the questions and actually handle the permits. So, save time and resources, and then to be able to allocate existing human resources into tasks that require more human attention' (Interviewee 4).

SIS will help municipality staff so that they are not restricted by time or workload constraints. Interviewee 4 also proposed that in the future, if they had access to more citizens' data, it may allow the municipality to use other forms of SIS to intervene in circumstances where citizens risk falling into poverty. There is the possibility of helping them prevent this in advance, by using SIS and predictive algorithms. In addition to reducing inequality locally, some of the interviewees hoped that their projects could be used in other cities, as well. Interviewee 1 also stated that Amsterdam is working with other smart cities in their development of technology and innovative practices, both nationally and abroad. However, it is important that the transferral and use of data take privacy concerns into account.

4.4. Privacy and Data Ownership

Amsterdam is involved in a number of European projects, such as Decode, which unites a range of different stakeholders and smart cities to develop innovative ideas to progress their projects. One of the main focuses of this project is to allow citizens greater control over their personal data and to ensure their privacy.

Interviewee 1 elaborated that this is a very important factor for all of her colleagues working on SIS in the city of Amsterdam – that people have control over their own data. It is a given that all of her colleagues work with privacy concerns in the back of their mind when using SIS. They also ensure that people cannot be traced using their SIS because they only analyse areas when they have a minimum number of people, whereby it is impossible to identify individuals amongst the group. Interviewee 1 stated that when they retrieve data from a certain area, they will always ensure that there it is a large number of people to ensure that their data is not traceable to a particular individual.

In contrast to Amsterdam's approach, Interviewee 2 claimed that personal data never ended up on their portal, so privacy was not an issue. They were GDPR compliant almost a year before the policy came into effect and they follow it strictly in order to fulfil its requirements. He also mentioned that they had an onus of responsibility to ensure that they were GDPR complaint. He stated that

'GDPR compliance was the responsibility of the suppliers, [...] they signed an agreement in which they stated they would be GDPR compliant' (Interviewee 2).

Similarly, Interviewee 3's MySMARTLife only dealt with data that has no locational or personal aspects to it. The project only uses 'object data'; for example, data retrieved from lamp posts and waste disposal machines.

'The second level [personal data] is definitely coming but it will be and has to be handled in a different way this is a subject to be tackled as well and will have some more obstacles to be overcome' (Interviewee 3).

However, in the follow-up interview, Interviewee 3 clarified that if this data were obtained, there would be explicit consent from the individuals, and their data would be anonymised. While Helsinki's chat-bot project retrieves the name, address, and vehicle registration number, from citizens looking for parking permits, Interviewee 4 indicated that the goal is that

'information would be stored in your citizen profile. And if you want, any time, you can log into your profile, see what data the city has about you, where it has been used, and you can give your consent to use it elsewhere, take it out, et cetera. But basically, you control it' (Interviewee 4).

There is a strong emphasis on the citizens owning and controlling their data and personal information and consenting to its use. Interviewee 4 states that it would be unethical for a state to use citizens' data to intervene in their lives without their consent. However, it is also important to identify who has control over data in public-private smart city projects. For example, Interviewee 2 mentioned that

'only Hitachi had control over the data once they were published on the portal' (Interviewee 2).

Therefore, there is a need for transparency and involvement between partners in order to ensure a fair and equitable interaction within smart city projects. While private organisations may be best suited to control and manage SIS, there needs to be an understanding between partners and a strong degree of transparency in their relationship.

4.5. Transparency and Trust

In the City Data Exchange project, Interviewee 2 elaborated that transparency was not an issue in the City Data Exchange project because the systems and methods being used were very simple and the project did not try to conceal anything about how it functioned. While Interviewee 3 stated that there has to be a symbiotic relationship of trust between corporations, citizens and municipalities working on Smart City projects. He also mentioned the transparency law of the City of Hamburg, which requests by law that all city data is openly accessible and availability and this has been considered in MySMARTLife.

Interviewee 3 also mentioned that there is a transparency law which necessitates that some of the data needs to be publicly available or officially provided on the website, for their project in Hamburg. Interviewee 4 also understands that incorporating SIS within city contexts requires a great deal of trust from citizens for these technologies to be adapted successfully:

'And it's a very delicate trust issue' (Interviewee 4).

In the chat-bot project in Helsinki, they also aimed to be transparent to citizens, showing that they were not speaking with a human, but a bot:

'clearly explaining to people that, "You are now talking to a chat-bot"' (Interviewee 4).

Interviewee 1 also said that transparency and trust were important issues for Amsterdam municipality:

'you might want to make it transparent for all citizens', and she hopes that 'citizens trust our municipal as well as the city already' (Interviewee 1).

Interviewee 1 claimed that those creating and using algorithms should be accountable for the choices that they make:

*‘So, it’s our duty then, our responsibility to make sure that the algorithms are working’
(Interviewee 1).*

5. Conclusion

This case study has offered many insights into the development, use and implementation of SIS technologies within smart city contexts in order to uncover ethical and social issues throughout these approaches.

We analysed four different organisations in order to retrieve an inclusive, varying look at how cities, semi-state bodies, and corporations develop and integrate SIS technologies in four major European cities (Amsterdam, Copenhagen, Hamburg, and Helsinki). The four interviewees were involved in varying projects, so we were interested to see if they had divergent concerns or if there were consistent overlapping ethical themes throughout. For instance, Interviewee 1 (Amsterdam) discussed her work on an Natural language processing (NLP) citizen complaint technology; Interviewee 2 (Copenhagen) spoke about sharing large datasets; Interviewee 3 (Hamburg) concentrated on an open standardized platform using smart energy and smart mobility solutions, and Interviewee 4 (Helsinki) discussed an AI customer-service chat-bot.

The level of public-private discussion throughout the four interviews was also very interesting, with a wide range of different approaches throughout. Amsterdam is attempting to implement SIS independently from corporate involvement, as much as possible. The data-sharing project in Copenhagen hired Hitachi to assist them, and the project in Helsinki used IBM Watson in-house but hoped to involve tech corporations in the future. While Interviewee 3 who is working on the project in Hamburg is employed by Deutsche Telekom, a large multinational German telecommunication provider. Throughout all four interviews, they highlighted the need to have a transparent relationship between public and private sectors in smart city development.

The diversity of interviewees and projects allowed for a diverse and informative mix of approaches and viewpoints for our case study. All four interviewees identified a range of ethical issues pertaining to their particular projects, with a great deal of overlap and similar issues being faced throughout. There was a great deal of similarity between organisations, particularly in relation to their concern and protocol for dealing with privacy concerns; understanding of the importance of accurate available data; economic concerns with implementing SIS; and ensuring trust and transparency to the general public. However, interviewing four different organisations also created limitations for our case study.

5.1. Limitations

One of the main limitations of this case study is that it was based on only four interviewees from separate organisations. Each interviewee was very knowledgeable about SIS and their societal and ethical impacts, the case study would have been improved by additional interviews in each organisation. While it was interesting and useful to incorporate a wide diversity of SIS, organisations, and smart city projects, it was a limiting factor when comparing them.

The case study focused on a few very specific applications of SIS within municipalities (chat-bots, SIS research project, SIS complaints procedure, and Big Data sharing), making it impossible to establish broader deductions about SIS in smart cities, generally. Also, each organisation adopted divergent approaches to ethical issues because of the different types of SIS being used. One example of this is their approach to citizen engagement: Amsterdam actively pursues citizen focus groups,

MySMARTLife and the Helsinki project only integrate citizen feedback in the use stage, while Copenhagen had very little citizen engagement at all.

An additional limitation resulted from discrepancies in relation to their concern about certain ethical issues, such as their reason for being concerned about transparency (interviewee 1 – obligation to citizens, interviewee 2 – it was a non-issue, interviewee 3 – obliged by Hamburg law, interviewee 4 – acceptability requires transparency). Therefore, it was difficult to form a cohesive understanding for broader assumptions about the implementation of transparency in smart city projects. Furthermore, all four projects were at different stages of development, making it difficult to compare their successes and failures. For example, Helsinki's chat-bot and Amsterdam's SIS project is in its early stages of development, while Hamburg's MySMARTLife project is matured, and the Copenhagen project has ceased.

A further limitation came from the knowledge and expertise of the interviewers. The interviews were evenly shared between two interviewers with different backgrounds and approaches. One interviewer is an ethicist and the second is a cultural anthropologist, which may have led to different focuses of the interviews, namely, a concentration on ethical issues or social dimensions, respectively. While both had interview experience, only the latter had a background in process of social science interviews.

5.2. Contribution to Knowledge

While there have been case studies on smart cities before, they have been few in number, mostly non-European cities, and with little focus on SIS (Bakıcı, Almirall, and Wareham 2013; Hielkema and Hongisto 2013; Lee and Gong Hancock 2012; and Mahizhnan 1999). This case study offers an innovative analysis of smart cities by analysing organisations not been discussed in the literature. This report provides fresh insights into the field of SIS in urban European contexts and how developers are approaching the ethical implementation of such technologies. While smart cities are discussed, evaluated, and critiqued within the field, there is rarely any detailed, specific analysis of the ethical implications of using SIS within smart city projects. This report offers theoretical value to the field of smart city knowledge, to urban SIS technology understandings, and to SIS ethics literature.

The interviews contained elements that were not addressed, or at least were given minimal attention, in the literature on smart cities, such as transparency and trust. While these are popular topic within data circles, they were not explicitly discussed in any smart city SIS literature. This report will greatly contribute to the debate by providing insights from four smart city projects and how they approach the issue of trust and transparency, which will contribute to the literature on these topics.

Another issue is that the literature deals with the smart city concept and how it impacts the meaning of the city, which are too broad for individual smart city projects. While the interviewees discussed most of the topics in the literature (such as privacy, transparency and trust), they did not draw out issues such as the digital divide between cities, countries, and rural areas. It became evident that there is a tension between theoretical concerns and those faced by people working 'on-the-ground'. The literature often concentrates on future-focused issues that may not even materialise, whereas smart city projects are more concerned with pragmatic tangible issues. Furthermore, it was shown that municipality SIS projects are primarily concerned with the impact of SIS on their citizens, rather than other groups within society.

5.3. Implications of this Report

Smart cities are a new development (first coined in 2008), along with the integration of SIS in urban contexts, so it is important to understand what kind of implications this will have on citizens' day-to-day lives and society as a whole. So far, there has been little policy to regulate SIS use in smart city projects, so this report hopes to offer unique feedback for future policy developments. Therefore, the effects of using SIS within smart city projects have not yet materialised, because of their infancy. While all four projects emphasised that their technologies had minimal-to-no harmful effects on the lives of citizens, this is not to say that more disruptive technologies will not be advanced in the future, making it vital that smart city projects continue to integrate ethical principles and approaches to avoid potentially harmful impacts.

As the case study gathered information from a variety of sources, conclusions from the comparison of these case studies can potentially be applied to other smart cities pilot projects. One such implication was the inclusion of citizen engagement in many of the projects – Amsterdam's Demo Thursday, Helsinki's apps for customers to lodge feedback, and Hamburg's citizen engagement project mandate. Engaging citizens remains problematic for many projects but towards engaging citizens more in the smart city planning and execution processes, these projects demonstrate a positive move away from the corporate agenda towards a citizen-centred one.

It should also be noted that across all of the projects the importance of privacy, trust, transparency and compliance to laws such as GDPR were paramount. Methods to maintain the privacy of data were: anonymized and aggregated Data (Helsinki and Hamburg), GDPR compliance on the part of those who deliver the data (Copenhagen). Applications of transparency became apparent through the chat-bot in Amsterdam, which explained clearly that it was a bot, and in Hamburg under the transparency law, but remained more abstract for the other projects. Trust, on the other hand, being subjective is 'a very delicate issue' (Interviewee 4) and although being an 'important issue' has fewer concrete actions attached to it.

In addition, our case study will have implications for policy development in the areas of ethical use of SIS in smart cities of the future. There has been very little guidance on how to effectively and ethically implement SIS in smart cities within policy frameworks and guidelines, particularly in a European context. While there are many more general guidelines relating to AI use, privacy protection, cybersecurity protocols, and so forth; there are few frameworks for municipalities to follow when adapting and pioneering SIS technology within their cities. However, this is not to say that additional case studies on the ethical use of SIS in smart cities will not find different issues and bring new perspectives to the debate.

5.4. Further Research

This case study has provided a literature review of some of the most important ethical and social issues within the field of smart city SIS technologies, it was also used as an overview to lend credence to our evaluations of the four organisations that we interviewed. There may be additional ethical issues within the literature, or that may arise in the coming years, that need to be evaluated and discussed. However, there is a distinct lack of empirical research done on smart cities, specifically analysing how they ethically use SIS technologies.

There is a need for more case study reports on smart cities generally, and more specifically, on European-based projects and smart city projects heavily involved integrating SIS technology. It may also be interesting to conduct further research on the projects discussed in this report at a future date to examine their progress and if they were successfully implemented. Overall, this case study hopes to offer a fresh examination of this topic, laying the groundwork for further research to be done in this area.

6. References

- Albino, Vito, Umberto Berardi, and Rosa Maria Dangelico, "Smart Cities: Definitions, Dimensions, Performance, and Initiatives", *Journal of Urban Technology*, Vol. 22, Issue 1, 2015, pp. 3-21.
- Bakıcı, Tuba, Esteve Almirall, and Jonathan Wareham, "A Smart City Initiative: The Case of Barcelona", *Journal of the Knowledge Economy* Vol. 4, Issue 2, 2013, pp. 135-148.
- Bartoli, A., J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Security and Privacy in your Smart City", *Proceedings of the Barcelona Smart Cities Congress*, Vol. 292, 2011, pp. 1-6.
- Batty, Michael, Kay W. Axhausen, Fosca Giannotti, Alexei Pozdnoukhov, Armando Bazzani, Monica Wachowicz, Georgios Ouzounis, and Yuval Portugali, "Smart Cities of the Future", *The European Physical Journal Special Topics*, Vol. 214, Issue 1, 2012, pp. 481-518.
- Brokaw, Leslie, "Six Lessons From Amsterdam's Smart City Initiative", *Sloan Review*, May 25th 2016, <https://sloanreview.mit.edu/article/six-lessons-from-amsterdams-smart-city-initiative/>
- Chourabi, Hafedh, Taewoo Nam, Shawn Walker, J. Ramon Gil-Garcia, Sehl Mellouli, Karine Nahon, Theresa A. Pardo, and Hans Jochen Scholl, "Understanding Smart Cities: An Integrative Framework", *45th Hawaii International Conference on System Science (HICSS)*, 2012, pp. 2289-2297.
- Condliffe, Jamie, "AI Has Beaten Humans at Lip-reading", *Technology Review*, November 21st 2016, <https://www.technologyreview.com/s/602949/ai-has-beaten-humans-at-lip-reading/>
- Copenhagen Solutions Lab, "Contact: Interviewee 2", *CPH Solutions Lab* [website], 2018, available here: <https://cphsolutionslab.dk/en/people/frans-la-cour>
- Daalder, Leonieke, "Ger Baron (CTO of the Municipality of Amsterdam): 'How do we go from Government to GovTech?'", Marketing Facts, 6th March 2018: <https://www.marketingfacts.nl/berichten/ger-baron-cto-gemeente-amsterdam-overheid-govtech>
- Deutsche Telekom, "At a Glance", *Deutsche Telekom* [website], retrieved November 6th 2018, available here: <https://www.telekom.com/en/company/at-a-glance>
- European Commission, "The Digital Economy and Society Index", *European Commission* [website], 2018, available here: <https://ec.europa.eu/digital-single-market/desi>
- Finn, Rachel L., David Wright, and Michael Friedewald. "Seven Types of Privacy", *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 3-32.
- Foth, Marcus, "The Software-Sorted City: Big Data & Algorithms", Odendaal, Nancy and Alessandro Aurigi (Eds.), *Digital Cities 10: Towards a Localised Socio-Technical Understanding of the 'Real' Smart City*, 26 June 2017, Troyes, France, 2017.
- Galdon-Clavell, Gemma, "(Not So) Smart Cities?: The Drivers, Impact and Risks of Surveillance-Enabled Smart Environments", *Science and Public Policy*, Vol. 40, 2013, p. pp. 717-723.

- Glasmeier, Amy, and Susan Christopherson, "Thinking About Smart Cities", *Cambridge Journal of Regions, Economy and Society*, Vol. 8, 2015, pp. 3-12.
- Guo, Kun, Yueming Lu, Hui Gao, and Ruohan Cao, "Artificial Intelligence-Based Semantic Internet of Things in a User-Centric Smart City", *Sensors*, Vol. 18, Issue 1341, 2018, pp. 1-22.
- Harris, Mark, "AI-Powered Body Scanners Could Soon Be Inspecting you in Public Places", *The Guardian*, 2nd October 2016, 2016,
<https://www.theguardian.com/technology/2016/oct/25/airport-body-scanner-artificial-intelligence>
- Helsinki Smart Region, "About: Helsinki Region", *Helsinki Smart Region* [website], 2018a, available here: <https://www.helsinkismart.fi/about/about-helsinki-region/>
- Helsinki Smart Region, "Why Finland and Why the Helsinki Region?", *Helsinki Smart Region* [website], 2018b, available here: <https://www.helsinkismart.fi/about/top-rankings/>
- Hielkema, Hendrik, and Patrizia Hongisto, "Developing the Helsinki Smart City: The Role of Competitions for Open Data Applications", *Journal of the Knowledge Economy* Vol 4, Issue 2, 2013, pp. 190-204.
- Hollands, Robert G. "Critical Interventions into the Corporate Smart City", *Cambridge Journal of Regions, Economy and Society*, Vol. 8, Issue 1, 2015, pp. 61-77.
- Kitchin, Rob, "Big Data and Human Geography: Opportunities, Challenges and Risks", *Dialogues in Human Geography*, Vol. 3, Issue 3, 2013, pp. 262-267.
- Kitchin, Rob, "Data-Driven Networked Urbanism", *The Programmable City Working Paper 14*, 10th August 2015, 2015a.
- Kitchin, Rob, "Getting Smarter about Smart Cities: Improving Data Privacy and Data Security", *Data Protection Unit*, Department of the Taoiseach, Dublin, Ireland, 2016a.
- Kitchin, Rob, "Reframing, Reimagining and Remaking Smart Cities", *The Programmable City Working Paper 20*, 16th August 2016, 2016b.
- Kitchen, Rob, "The Ethics of Smart Cities and Urban Science", *Phil. Trans. R. Soc. A*, Vol. 374, 2016c, pp. 1-15.
- Kitchin, Rob, "The Promise and Perils of Smart Cities", *Society for Computers & Law*, Vol. 26, Issue 2, 2015b, pp. 1-5.
- Kitchin, Rob, "The Real-Time City? Big Data and Smart Urbanism", *GeoJournal*, Vol. 79, 2014, pp. 1-14.
- Kitchin, Rob, Claudio Coletta, Leighton Evans, Liam Heaphy and Darach Mac Donncha, "Smart Cities, Urban Technocrats, Epistemic Communities and Advocacy Coalitions", *The Programmable City Working Paper 26*, 8th March 2017, 2017.
- Kitchin, Rob, Tracey P. Lauriault, and Gavin McArdle, "Smart Cities and the Politics of Urban Data", *Smart Urbanism: Utopian Vision or False Dawn?*, Routledge, London, 2015, pp. 16-33. ISBN 9781138844223.

- Kohli, Devika, "How Smart Cities Will Force the Poor Out", *Youth Ki Awaaz* [website], 2014, available here: <https://www.youthkiawaaz.com/2015/07/smart-cities-keep-the-poor-out/>
- Lee, Jung-Hoon, and Marguerite Gong Hancock, "Toward a Framework for Smart Cities: A Comparison of Seoul, San Francisco and Amsterdam", *Research Paper, Yonsei University and Stanford University*, 2012.
- Li, DeRen, JianJun Cao, and Yuan Yao, "Big Data in Smart Cities", *Science China Information Sciences*, Vol. 58, Issue 10, 2015, pp. 1-12.
- Macpherson, Lauren, "8 Years On, Amsterdam is Still Leading the Way as a Smart City", *Towards Data Science*, 7th September 2017, <https://towardsdatascience.com/8-years-on-amsterdam-is-still-leading-the-way-as-a-smart-city-79bd91c7ac13>
- Mahizhnan, Arun, "Smart Cities: The Singapore Case", *Cities* Vol. 16, Issue 1, 1999, pp. 13-18.
- Martínez-Ballesté, Antoni, Pablo A. Pérez-Martínez, and Agusti Solanas, "The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City is Possible", *IEEE Communications Magazine*, Vol. 51, Issue 6, 2013, pp. 136-141.
- The Municipality of Copenhagen and Capital Region, "City Data Exchange – Lessons Learned From A Public/Private Data Collaboration", *CPH Solutions Lab* [website], March 2018, available here: <https://cphsolutionslab.dk/content/2-what-we-do/3-data-platforms/3-city-data-exchange/1-learnings-from-the-city-data-exchange-project/city-data-exchange-cde-lessons-learned-from-a-public-private-data-collaboration.pdf?1527149474>
- Munoz, Mark J., Al Naqvi, "Artificial Intelligence and Urbanization: The rise of the Elysium City", *Economics and Political Economy*, Vol. 4, Issue 1, March 2017, pp. 1-13.
- MySMARTLife, *MySMARTLife* [website], 2018a, available here: <https://www.mySMARTLife.eu/mySMARTLife/>
- MySMARTLife, "An Integrated Planning Process, Where Citizens are Actively Involved in the Decision-Making", *MySMARTLife* [website], 2018b, available here: <https://www.mySMARTLife.eu/mySMARTLife/>
- Nigon, Julien, Estèle Glize, David Dupas, Fabrice Crasnier, Jérémy Boes, "Use Cases of Pervasive Artificial Intelligence for Smart Cities Challenges", *IEEE Workshop on Smart and Sustainable City (WSSC 2016) associated to the International Conference IEEE UIC 2016*, Toulouse, France, July 2016.
- O'Grady, Michael, and Gregory O'Hare, "How Smart is Your City?", *Science*, Vol. 335, Issue 6076, 2012, pp. 1581-1582.
- Owen, Richard, Jack Stilgoe, Phil Macnaghten, Mike Gorman, Erik Fisher, and Dave Guston. 2013. "A Framework for Responsible Innovation." In *Responsible Innovation*, edited by Richard Owen, John Bessant, and Maggy Heintz, 27–50. London: John Wiley.
- Rjab, Amal Ben, and Sehl Mellouli, "Smart Cities in the Era of Artificial Intelligence and Internet of Things: Literature Review from 1990 to 2017", *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, May 30-June 1, 2018, Delft, Netherlands, ACM, 2018.

- Roose, Jonatan, "About Amsterdam Smart City", Amsterdam Smart City [website], 2015, <https://amsterdamsmartcity.com/p/about>
- Shelton, Taylor, Matthew Zook, and Alan Wiig, "The 'Actually Existing Smart City'", *Cambridge Journal of Regions, Economy and Society*, Vol. 8, Issue 1, 2015, pp. 13-25.
- Sholla, Sahil, Roohie Naaz, and Mohammad Ahsan Chishti. "Ethics Aware Object Oriented Smart City Architecture", *China Communications*, Vol. 14, Issue 5, 2017, pp. 160-173.
- Srivastava, Shweta, Aditya Bisht, and Neetu Narayan, "Safety and security in smart cities using artificial intelligence—A review", *Data Science & Engineering-Confluence, 2017 7th International Conference on Cloud Computing*, IEEE, 2017, pp. 130-133.
- Tung, Liam, "Google AI Can Pick Out a Single Speaker in a Crowd: Expect To See it in Tons of Products", *ZDNet* [website], April 13th 2018, <https://www.zdnet.com/article/google-ai-can-pick-out-a-single-speaker-in-a-crowd-expect-to-see-it-in-tons-of-products/>
- Vázquez-Salceda, Javier, Sergio Álvarez Napagao, José Arturo Tejeda Gómez, Luis Javier Oliva Felipe, Dario Garcia Gasulla, Ignasi Gómez Sebastià, and Víctor Codina Busquet, "Making Smart Cities Smarter Using Artificial Intelligence Techniques for Smarter Mobility", in *SMARTGREENS 2014: proceedings of the 3rd International Conference on Smart Grids and Green IT Systems*, pp. IS7-IS11. SciTePress, 2014.
- Voda, Ana Iolanda, and Laura Diana Radu, "Artificial Intelligence and the Future of Smart Cities", *Broad Research in Artificial Intelligence and Neuroscience*, Vol. 9, Issue 2, 2018, pp. 110-127.
- UNESCO Institute for Statistics, "R&D Spending by Country", *UNESCO* [website], 2018, available here: <http://uis.unesco.org/apps/visualisations/research-and-development-spending/>
- United Nations, "Goal 11: Make Cities Inclusive, Safe, Resilient and Sustainable", *UN* [website], 2018, available here: <https://www.un.org/sustainabledevelopment/cities/>
- Zanella, Andrea, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi, "Internet of Things for Smart Cities", *IEEE Internet of Things Journal*, Vol. 1, Issue 1, 2014, pp. 22-32.
- Zhang, Kuan, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin Sherman Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions", *IEEE Communications Magazine*, Vol. 55, Issue 1, 2017, pp. 122-129.

CS05 – Science



Case Study: Ethical Reflections of Human Brain Research and Smart Information Systems



**This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641**



Document Control

Deliverable	D1.1 Case Studies
WP/Task Related	WP 1: Representation and Visualisation
Delivery Date	31 January 2019
Dissemination Level	Public
Lead Partner	De Montfort University
Contributors	Tilimbe Jiya, De Montfort University Bernd Stahl, De Montfort University
Reviewers	Kevin Macnish, UT; Mark Ryan, UT
Abstract	
Key Words	Smart information systems, responsible research and innovation, ethics, human brain research

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes

Contents

Contents	145
Executive Summary	146
1. Introduction	147
2. The use of SIS in Human Brain Research	147
3. Ethical Issues with SIS in Human Brain Research	149
3.1 Privacy	149
3.2 Data ownership	150
3.3 Trust and Accountability	150
4. Human Brain Project: A Case of a project that uses SIS in Brain Research	150
4.1 Individuals Interviewed	151
4.2 The SIS being used by the Human Brain Project	152
4.3 The aims of the HBP in using SIS	155
4.3.1 Data manipulation	155
4.3.2 Virtualisation	155
4.3.3 Data exploitation	155
4.4 The Effectiveness and Impact of the SIS	156
5. Ethical Issues with the use of the SIS	158
5.1 Privacy and Confidentiality	158
5.2 Personal Data and Security	159
5.3 Discrimination and Bias	160
5.4 Transparency	161
5.5 Mechanisms to Address Ethical Issues	161
6. Conclusion	163
6.1 Limitations	164
6.2 Contribution and Implication of this Case study	164
6.3 Further Research: bio-AI, see opening comments	165
7. References	165

Executive Summary

This report presents a case study on the ethical issues that relate to the use of Smart Information Systems (SIS) in human brain research. The case study is based on the Human Brain Project (HBP) which is a European Union funded project. The project uses SIS to build a research infrastructure aimed at the advancement of neuroscience, medicine and computing. The case study was conducted to assess how the HBP recognises and deal with ethical concerns relating to the use of SIS in human brain research. In order to understanding some of the ethical implications of using SIS in human brain research, data was collected through a document review and three semi-structured interviews with participants from the HBP. The document review included an analysis of the literature on ethical issues with the use of SIS in human brain research, the project's website and project deliverables.

Results from the case study indicate that the main ethical concerns with the use of SIS in human brain research include privacy and confidentiality, security of personal data, discrimination that arises from bias and access to the SIS and their outcomes. Furthermore, there is an issue with the transparency of the processes that are involved in human brain research. In response to these issues, the HBP has put in place different mechanisms to ensure responsible research and innovation through a dedicated program. The dedicated program includes a Foresight Lab, Ethics Support, Ethics Rapporteur Programme, a Data Protection Officer, public engagement, Neuroethical reflection, Ethics Advisory Board and a Data Governance Working Group.

This case study report is important because it provides lessons for the responsible implementation of SIS in research, including human brain research. The report acknowledges the ethical issues that relate to the use of SIS in human brain research and puts forward some of the mechanisms that could be employed by researchers and developers of SIS for research in addressing such issues.

The report has some limitations regarding the range of the identified ethical issues. Given the size of the HBP, it would be ideal if there could be a wider exploration of different views on the ethical issues across the multiple roles involved in different SIS platforms within the HBP. Such a limitation calls for a further study at a later stage of the project to get more perspectives. Nevertheless, the case study gives a starting point for reflecting on the ethical considerations of human brain research and SIS by revealing some of the current ethical issues. Thus, it lays a foundation for anticipating on future issues with the use of SIS in human brain research and how to address them.

1. Introduction

Considerable research is undertaken on the use of innovative computer technologies in understanding the human brain (Goertzel et al., 2010; Shapshak, 2018). One example of such research is the Human Brain Project (HBP), a ten-year scientific research project that aims to build an ICT infrastructure for neuroscientific research. Various components of this large and complex project involve Artificial Intelligence (AI) and Big Data (Smart Information Systems - SIS). The HBP aims to build a collaborative ICT-based scientific research infrastructure to allow researchers across Europe to advance knowledge in the fields of neuroscience, computing, and brain-related medicine (Human Brain Project, 2018).

In general, the use of such SIS raises ethical concerns relating to autonomy, trust, consent, identification, inclusion and digital divides, security, harm, misuse, and deception, to name just a few (Stahl and Wright, 2018). Drawing from the research in the HBP, this report presents an analysis of ethical issues arising from the use of SIS in human brain research. Using a case study of the HBP, it covers insights from the project to reinforce the comprehension of well-known ethical issues and possibly those that are not well known. In so doing, the case study addresses the research question: **how do organisations perceive ethical concerns related to SIS and in what ways do they deal with them?** To address the research question, data was collected through a document review and semi-structured interviews with three participants from the HBP. The structure of the report is as follows:

- Firstly, the report presents a review of the current use of SIS in human brain research focussing on the types of SIS technologies being used.
- Secondly, the report highlights a range of ethical issues surrounding the use and implementation of SIS in human brain research that are drawn from the literature.
- Thirdly, the report describes the HBP case. It outlines the SIS that are being used in the HBP and the aims of their use. Further, the report discusses the effectiveness of the SIS used in the HBP.
- Fourthly, the report presents the ethical issues that arise when using SIS technologies in HBP. This is followed by a discussion of the mechanisms that are used in the HBP to recognise and address ethical issues.

The report contributes to knowledge around the ethical use of SIS in human brain research. It also contributes to practice by looking at how SIS could be effectively and ethically implemented in human brain research. Thus, the report has implications on the formulation of policies to ensure that ethical and legal implementation of SIS in human brain research.

2. The use of SIS in Human Brain Research

Research on how the human brain functions has a long history. Humans have tried to understand what it is to remember, to reason and to know for a long time (Arbib, 1975). Today, this quest includes research to understand the human brain using computer

technologies. The human brain is a complex organ. Due to its complexity, scientists are trying to use the capabilities of some advanced SIS to discover and develop systems that can advance knowledge in the fields of neuroscience, computing, and brain-related medicine. Research into the brain is partly motivated by the rise in brain diseases as people have longer lifespans, and at the same time have to adapt to an ever more complex society. These changes in society and life have provided new reasons to study the brain, and more scientists are now keen to research and develop technologies that can support brain research (Goertzel et al., 2010).

In view of that, there is ongoing research that uses science and technology based on a comprehensive understanding of the structure and behaviour of matter from the Nano-scale up to the most complex system yet discovered, the human brain (Shapshak, 2018). Part of that research has seen concentrated efforts to bring together information technology with new technologies based on cognitive science to understand how the brain functions. The benefits of such convergence have the potential to improve a better examination of biological intelligence and understand how the brain functions (Hassabis et al., 2017).

The use of technologies such as SIS in human brain research has been going on for many years. Many studies have been conducted to develop technologies that help in delving deep into the functions of the brain and learn the principles that are fundamental to its design and operation (Huerta et al., 1993; Shepherd et al., 1998). Neuroinformatics³⁷, which allows scientists to collect and organise huge volumes of data on the brain, has been a catalyst of a rise in the use of SIS in human brain research (Alexiou et al., 2013; INCF, 2018). The use of SIS in this regard is aimed at exposing correlations and other patterns in data and in extracting general organising principles. Examples of such use can be seen in initiatives such as the International Neuroinformatics Coordinating Facility (INCF)³⁸, The Human Connectome Project³⁹, and The Brain Research through Advancing Innovative Neurotechnologies (BRAIN) Initiative⁴⁰.

In most research initiatives on the human brain, there is use of new enabling technologies such as modern High-Performance Computing (HPC) and simulation-based science (Reger et al., 2000), which are now combined with Big Data analytics and AI to provide powerful SIS. Over the years the use of SIS in human brain research has progressed (Goertzel et al., 2010; Prieto et al., 2016; Reger et al., 2000), and recent advanced SIS systems have been used to model and simulate brain processes and thus reveal the complex chains of causation leading from cells and connections, to behaviour and cognition (Shapshak, 2018).

With the use of SIS, brain simulations can organise data and knowledge to allow researchers to address the ultimate questions concerning the origins of cognition and behaviour. As SIS

³⁷ A research field concerned with the manipulation of neuroscience data through the use of computational models and analytical tools.

³⁸ INCF, Advancing data reuse and reproducibility in global brain research. <https://www.incf.org/about>

³⁹ The Human Connectome Project (HCP). <http://www.humanconnectomeproject.org/about/>

⁴⁰ What is the brain initiative? <https://www.braininitiative.nih.gov/>

advance, they will continue to be a key enabling technology for new approaches to brain research, and the knowledge that results from their use will promote a completely new class of information systems.

At the heart of these new information systems is the influence of neuroscience on SIS. Using technologies such as neural networks and deep learning, SIS have been adopted to understand the functions of the brain. AI and Big Data have been revolutionised by remarkable advances in neural network or deep learning methods (LeCun et al., 2015; Prieto et al., 2016). Core to such an understanding are the insights that are cultivated from neuroscience. Neuroscience provides a rich source of inspiration for new types of algorithms and architectures, independent of and complementary to the mathematical and logic-based methods and ideas that have largely dominated traditional approaches to AI (Hassabis et al., 2017).

Although this sounds promising, there are ethical issues related to the use of SIS in human brain research. These are covered in the following section.

3. Ethical Issues with SIS in Human Brain Research

The use of SIS in human brain research raises several ethical issues. During background research into the ethical issues of using SIS in human brain research, a number of sources were used. These sources included journals such as IEEE Security Privacy, Neuron, and The Journal of Supercomputing. Also, insights were derived from Artificial Intelligence Applications and Innovations (AIAI) international conference proceedings to further understand the ethical issues with SIS technologies. In coming up with relevant literature, a broad search of keywords using different variations was conducted in databases such as Google Scholar and Scopus. After reviewing these articles, a number of ethical issues with respect to the use of SIS in brain research such as privacy, data ownership, accountability and trust were established.

3.1 Privacy

In brain research, SIS pose a risk of violating privacy through the actions and rules that define who has access to certain types of information. There is also a risk of discovering the data providers' identity, or disclosure of sensitive information. For instance, there is wide use of global repositories that are populated by data, and protocols which are prone to the risk of intrinsic and consequential harm of the data owners or research participants (Stahl and Wright, 2018). The repositories contain data that could be re-identified to the primary source and violate their privacy. Although this is not straightforward, with advanced data aggregation and mining techniques, there is the possibility of re-identification of the data subjects (Rommelfanger et al., 2018).

3.2 Data ownership

There is a possibility that the data that are being used for research could be commercialised and shared with third parties for other purposes. This raises issues relating to data ownership and the intellectual property rights. Since human brain research involves massive unstructured data which is collected, stored and processed by the SIS used in the research, it involves complex ethical considerations because the big datasets may consist of a variety of intellectual properties, such as research results, copyrights, trademarks, and patents (Alexiou et al., 2013; Anagnostopoulos et al., 2016). The use of SIS in human brain research also raises the question of equitable access to the benefits of applications for the data subjects, such as patients, beyond the research itself (Rommelfanger et al., 2018).

3.3 Trust and Accountability

Another ethical issue relating to the use of SIS in brain research is that of trust and accountability. Trust of all the stakeholders in the use of SIS in brain research is important. There is a requirement of accountability that should be upheld by the researchers and other stakeholders, particularly when it comes to data manipulation, sharing, access to data, allocation of rights and ownership. Relatedly, the use of SIS also brings with it issues of algorithmic bias and the transparency of the decisions that are made by the artificial intelligence within the SIS (Stahl and Wright, 2018). In the case of human brain research, the use of Big Data poses ethical and policy-related issues concerning the governance and regulation of data content, access to and use of databases or datasets (Anagnostopoulos et al., 2016).

So far, the report has indicated that the use of SIS in brain research is not a new thing. Advanced technologies such as SIS are used to conduct research relating to the brain, and the use of AI and big data open new capabilities in trying to understand how the brain functions. Moving on, the next section will describe HBP, which implements and uses SIS in human brain research.

4. Human Brain Project: A Case of a project that uses SIS in Brain Research

The Human Brain Project (HBP) is building a research infrastructure to help advance neuroscience, medicine and computing. The HBP is a 10-year project that is funded by the European Union, which began in 2013. The project directly employs more than 800 people in over 100 universities, teaching hospitals and research centres in 20 countries around the

globe. The HBP aims to develop an ICT infrastructure for neuroscience (Amunts et al., 2016). It is a cutting-edge SIS project in several ways. It uses massive amounts of neuroscientific data and AI for the generation of new insights into the brain, and is developing novel computational architectures based on neuroscience that may overcome some of the limitations of current AI.

The HBP is structured around a unified agenda to gather and analyse data on the brain, derive organising principles and build brain models with as much biological detail as technically possible (Human Brain Project, 2018). The HBP will use the advancement of brain science and medicine to accelerate our understanding of the brain and its diseases. Such models represent extreme applications that will shape the future of supercomputing and provide the technologies to create realistic simulations of life processes. Combined with high-level mathematical theories of brain function, the HBP uses SIS in its quest to build a new class of brain-like hardware devices and computer architectures that may result in the next generation of AI and data analytics. However, the use of SIS in the HBP has ethical implications and it is important to understand these.

To understand some of the ethical issues with the use of SIS in human brain research, background research about the use of SIS in human brain research and its ethical implications was conducted. The results were presented above. Also, three interviews with members of the HBP were conducted to gain an in-depth understanding of their interactions with SIS and their views of the most fundamental ethical issues relating to the use of SIS in the project. The interviews were conducted between August and December 2018.

The data collected were analysed using a thematic data analysis technique which was both deductive and inductive. The deductive themes were derived from the interview questions to begin the analysis process. Using Nvivo qualitative data analysis software, categories were established into different nodes during a two-day SHERPA consortium workshop. Consequently, inductive themes emerged from the interview transcripts to inform this case study report.

4.1 Individuals Interviewed

To get an in-depth understanding of the ethical issues related to the use of SIS in the HBP, three individuals were interviewed. The roles of the individuals interviewed ranged from ethics and data governance to the technical management of the SIS. For instance, one of the individuals was involved with cataloguing the ethical issues that could result from the use of algorithms and machine learning related analytical tools within the HBP. In summary, Table 1 below shows the interviewees and their roles.

Interviewee	Role in the HBP	Date of Interview
Interviewee 1	Ethic rapporteur	23.08.2018
Interviewee 2	Ethics and data governance	02.10.2018
Interviewee 3	Technical management	19.10.2018

Table 1: Interviewee roles in HBP

4.2 The SIS being used by the Human Brain Project

The SIS being used in different parts of HBP involves, at a minimum, three dozen separate algorithms and machine learning techniques. These techniques are used in joint platforms that unify SIS tools to build complex data-driven brain models. The joint platforms involve neuro-robotic simulations and high-performance computing kernels to support brain simulations. These SIS are used in the project's joint platforms including Neuro-informatics, Brain Simulation, High-Performance Analytics and Computing, Medical Informatics, Neuromorphic Computing, and Neurorobotics. These platforms are described in Table 2 below.

Platform	Description
Neuroinformatics Platform	The Neuroinformatics Platform involves collecting, organising and making available a range of brain data. It provides services to search and access neuroscience data, data models and other resources through multi-level brain atlases. The platform manages curation process and data registration of different kinds of data from humans and images.
Brain Simulation Platform	The Brain Simulation Platform provides tools and models to facilitate the convergence between different modelling tasks. This supports a further understanding of brain structure and function. It is an accessible platform designed to reconstruct the brain through simulation, with a whole suite of software tools and workflows for collaborative brain research. The platform allows researchers to simulate models of the brain at multiple levels on supercomputers.
High-Performance Analytics and Computing Platform	The High-Performance Analytics and Computing (HPAC) Platform builds, integrates and operates the hardware and software components of the project's supercomputing, data and visualisation infrastructure, providing the necessary computing and storage resources for neuroscientific research. The HPAC has very high computational power to run large-scale simulation involving the large amounts of data produced.
Medical Informatics Platform	The Medical Informatics Platform (MIP) gives researchers the ability to access and analyse large amounts of clinical data. The data provide patterns which are used to develop new hypotheses about brain diseases. Also, the platform is used for developing an understanding of disease clusters and their signatures. Early achievements using the MIP include the identification of new subtypes of dementia and the first biological signatures for that disease, which allows a prognosis to be established before the onset of disease symptoms.
Neuromorphic Computing Platform	The idea behind the Neuromorphic Computing Platform is to make computers that use a similar architecture to that inspired by the human brain, which would make some computationally difficult energy-intensive tasks more

accessible (Interviewee 2). This involves a remotely accessible large-scale neuromorphic computing system. The computing systems are built from fast, energy-efficient devices that imitate the brain's physical process.

Neurorobotics Platform	The Neurorobotics Platform involves virtual and real robots and environments for testing brain simulations. In the platform, its users can plan, run and evaluate neuroscience experiments that use a public online research interface that involves using virtual robots connected to simulated brains.
------------------------	--

Table 2: A Summary of Platforms that use SIS in HBP

4.3 The aims of the HBP in using SIS

4.3.1 Data manipulation

Scientists require the support of enormous computing power and information systems that can manipulate the huge datasets that human brain research involves. As pointed out by Interviewee 2, part of the reason for the platforms' existence in the HBP is to make a unified system that collects and builds complex data-driven brain models based on huge datasets. SIS are also used by neuroscientists to collect data, then develop brain models based on these data, and simulate these models (Amunts et al., 2016; Human Brain Project, 2018).

4.3.2 Virtualisation

SIS are used to develop virtual brain models which are used in real or simulated robot bodies. The Neurorobotics Platform gives any simulated brain model its virtual or real "body" and explores how it controls movement, reacts to stimuli, and learns in a virtual environment. According to Interviewee 3, the idea of some of the systems, such as the Neurobotic Platform, is:

"to have an accessible platform designed to reconstruct the brain through simulation involving simulating brain models with a whole suite of software tools and workflows for collaborative brain research. The important thing about this is that it will allow, in theory, researchers to simulate models of the brain at multiple levels".

Also, the SIS are used to link a simulated brain to a robotic body to provide a powerful mechanism for testing the fidelity of the brain simulation.

4.3.3 Data exploitation

The HBP's Medical Informatics Platform (MIP) is intended to advance brain medicine by using computer science to allow researchers around the world to exploit medical data, regardless of where the data may be stored, and to create machine-learning tools that can search these data for new insights into brain-related diseases. Huge volumes of data are shared across thousands of hospitals around the world. Although medical researchers can access data in their own hospital relatively easily, normally access to data in other hospitals is much more difficult, as patient confidentiality, data protection and the incompatibility of Information Communication and Technology (ICT) systems become major considerations (Human Brain Project, 2018). The MIP offers ICT solutions which overcome these constraints while maintaining the confidentiality that is so important to the medical profession and the patients through data curation. To support this, Interviewee 3 pointed out that:

'it is quite an expensive process to extract information in a manual form, a manual approach. Therefore, they used SIS trained to understand and facilitate automatic classification and extraction of structured metadata records.

Also, machine learning applied to huge data sets offers the possibility of identifying new “disease signatures”. These are based on a broad range of factors, from the molecular level to the whole brain, and observable disorders of cognition and behaviour, which should pave the way for improved diagnosis and hence better treatment outcomes. This involves:

'a lot of separate algorithms and machine learning techniques that are being used in different parts of the HBP' (Interviewee 2).

4.4 The Effectiveness and Impact of the SIS

At the time of writing the case study, the use of SIS in the HBP was showing some effectiveness towards the reduction of labour hours. Interviewee 3 stated that the use of SIS in the HBP is

'meant to reduce the amount of labour required to share data, to make it a more streamlined process and more efficient'.

For instance, the interviewee said that the data curation process is quite expensive because it requires relatively a lot of time and energy and discussion between people to make things work. However, with the use of SIS, some of the issues have been drastically minimised. One constraint that was mentioned that affects its effectiveness is bias. Interviewee 3 suggested that bias can affect the quality of the outputs being carried out by the SIS.

In terms of impact, the SIS has demonstrated long-term global impacts:

'with global users of the infrastructure, and global contributors of data to various activities in the infrastructure. And the data is expected to potentially be used by people outside of Europe' (Interviewee 3).

It is clear that the impact of the SIS will go beyond the lifespan of the project, as suggested by Interviewee 2 who mentioned that the infrastructure for neuroscience innovation that is used in the project is visionary and will be used in the future. The SIS in the HBP will allow a lot more open science through sharing metadata across the globe.

However, although there is potential impact of the SIS use in the HBP, some of the platforms are yet to show their full potential. An example was given for the MIP, in which Interviewee 1 stated that:

'the impact is still quite small because we are still developing the platform, but the first steps we've made have allowed some promising results in terms of identifying some subpopulations of people with the same disease [...] because of availability and sharing

of data that is more complex and huge than what would have been accessed by institutions individually' (Interviewee 1).

As the project progresses, there is an expectation of some large-scale effects when more hospitals are using the platform and sharing data.

Despite the impacts of SIS in the HBP, some limitations and constraints affect its use. For example, Interviewee 3 mentioned that the MIP works in some cases but not in others. This is put down to the fact that it has not been widely deployed and the project has only carried out a proof of concept to test the functionality of the SIS at this point in time. Interviewee 3 further said that one constraint that could affect how the SIS will work beyond the proof of concept stage would be the availability of the resources needed to continue.

Another limitation is related to the quality of the input data set. The effectiveness of the SIS in doing their job will be affected by the quality of data input. For instance, Interviewee 1 stated:

'if you have a bias in the input dataset you expect to see biased classification'.

This is very important, since the use of one of the platforms (MIP) is sorting, organising and sharing data for reporting, which calls for efficiency in the process to ensure quality outputs.

However, despite these limitations, the work of the SIS in HBP is promising. As Interviewee 1 pointed out, they:

'can expect that the more metadata we collect, the better data the systems will have to learn from when they go to do their classification process in the future. So, it should get better with time and type of scenario.'

With time, the SIS will mature and improve as has been seen in some areas of the MIP. With MIP, the SIS use of deep learning is maturing, particularly the part that is being used for text classification and automatic semantic tagging.

Lastly, the SIS used in the HBP has a long-term impact on different stakeholders, including scientists, medical professionals, patients and the public, because it facilitates a better and improved understanding of the brain, which will lead to improved medication and science that is geared towards addressing health problems related to the brain. As confirmed by Interviewee 1, the SIS provide ways about:

'how we can improve the healthcare system and make it more efficient and more patient-oriented, moving towards precision medicine'.

5. Ethical Issues with the use of the SIS

From the three interviews that were conducted in this case study, the ethical issues that were established resonate with those in the literature. There is a broad intersection between the ethical issues that are covered in the literature and those that emerged from the interviews. The ethical issues with the use of SIS in the HBP included privacy and confidentiality, personal data and security, discrimination and bias and finally, transparency. These ethical issues are discussed below.

5.1 Privacy and Confidentiality

One of the issues with the use of SIS in the HBP relates to privacy. Since the SIS collect personal data, all three interviewees stated that there is a risk of violating the privacy of the ‘*data subjects*’. For instance, Interviewee 2 mentioned that depending on the type of SIS, there were different levels of risk to privacy, with some of them presenting higher degrees than others. The interviewee gave an example of the Neurorobotics Platform, which is extremely unlikely to cause problems with privacy, compared to the MIP. The interviewee mentioned that the risk to privacy causes tension between innovation and privacy’ because everybody has to worry about user and staff data, and ‘despite good funding in the HBP not everybody was necessarily budgeting for massive encrypted servers back in 2012 when the project was conceptualised initially.

Similarly, Interviewee 1 mentioned that the risk of identifying patients will remain because there is always the possibility of hackers accessing the data. One thing that could be done is continuously keeping in mind the priority to protect patients’ data and empowering people with their data. The interviewee further said that this would involve explaining to patients the value of data, how to handle it, protect or share data.

Despite the doubts on the ethical implications relating to privacy and the General Data Protection Regulation (GDPR), Interviewee 3 stated that one idea to address the issue of privacy would be:

‘to have a federated sort of platform where people can query it without violating the GDPR [...] without posing any risk to patient confidentiality, data security, or any other privacy aspects’.

There is also an ethical concern relating to violation of group privacy through the possibility of considering specific algorithms, as the origins of the data sources include heritage or biography. According to Interviewee 2, this is worrying because there could be ‘*ways in which different sets of data can potentially be recombined to [...] identify groups*’. Despite this concern, the interviewee mentioned that as a project, the HBP has an ethical imperative to research with veracity, and there are some legal frameworks around the use of the SIS that could be used to mitigate against loss of integrity.

5.2 Personal Data and Security

Related to the issue of privacy in the HBP is the use of personal data. Interviewee 2 pointed out that the use of personal data and the:

'potential use of big data analytics, present concerns about group-level harms and the privacy of users. The big issue with the use of SIS is to figure out how to find the right balance between sharing (personal) data for research and to have enough usability of this data, respecting the patients' and the citizens' privacy'.

In addition to this concern, there are issues of using anonymisation as one of the techniques to secure the data from being misused. Interviewee 2 stated that the project goes:

'all the way to anonymisation which then probably renders the data not usable. So, one way to avoid this is by using a lot of information which then presents a big risk of re-identifying patients' (Interviewee 2).

As a result, there is a risk of some researchers trying to *'find out a way to de-anonymise data'* (Interviewee 2), because there is a push to innovate more and more, which is of concern when it comes to the ethical use of the SIS. Reflecting on this issue, Interviewee 2 said that the HBP tries:

'to find the right balance between protecting and using the data for progress'.

Parallel to the use of personal data is the issue of security. Interviewee 2 stated that there is always an issue of security at the software level because the SIS is using the internet. With the use of the internet, the systems are opening ports into hospitals which means that there should be a lot of safeguards for specific parts of a specific server. The interviewee acknowledged that:

'some technologies might feel very helpful, but maybe they are too open to hacking and penetration'.

Interviewee 2 stated that *'guaranteeing 100% that there will be absolutely no way to re-identify a patient is not possible'*. But, he further said that the risk of hacking the SIS is low because if someone was interested in identifiable data, they would be better off accessing it on the hospital servers compared to the MIP. This reinforces the fact that the data used in the MIP are:

'a result of aggregated analysis rather than raw data which poses a very low risk' (Interviewee 2).

Having said that, there is an acknowledgement that all the SIS platforms present various security risks. However, as pointed out in the interviews, the levels of risks vary in that some platforms. For instance, Neurorobotics platforms are extremely unlikely to cause problems

with privacy compared to other platforms due the type of data used although they could be prone to hacking.

In connection with personal data, there is also an issue of informed consent. Since the use of SIS in the project involves collection and manipulation of personal data, a question was raised on informed consent. Interviewee 3 stated that they assume that there is implied consent from some data subjects because:

‘researchers involved in the production of the data have chosen to be involved in the curation process’.

However, this is not the case with each person individually because they may have been implicitly involved when someone shared the dataset, therefore *‘their attachment to the dataset would require consent’*. Despite making these two suggestions, the interviewee added that they could not tell whether this was acceptable, only acknowledge that there was a potential issue with informed consent.

5.3 Discrimination and Bias

Issues surrounding discrimination and bias are important when it comes to the use of SIS in general. This was also unveiled as a potential issue with the use of SIS in the HBP. Interviewee 2 showed concern over bias and digital division that would result in the use of SIS in the project. The interviewee’s concern was connected to the availability of resources across that project which could result in a digital divide between those who have the resources to use most of the platforms and those who cannot. Also, this was something that would result from the different platforms not being joined up as would have been expected. Therefore, with the lack of integration:

‘there is a lack of fairness regarding who fully utilises the SIS and who does not’ (Interviewee 2).

There is also potential to discriminate by drawing on datasets that are non-representative of particular stakeholders when using the SIS. This was suggested by Interviewee 2, who said that there is *‘a potential to miss out on neuro-diverse people’* because of where the data are being drawn from. As a result, there could be some stakeholders who are left out and are not represented or included. One of the ways of tackling the issue of discrimination, according to the interviewee, is perhaps to reflect on the *‘algorithms or machine learning procedures’* that are being used in the project. This is also related to having open and transparent processes where people can ask questions around data sources and intentions with the aim to identify areas that are being overlooked.

5.4 Transparency

The SIS in the project uses several algorithms, but due to the nature of the project:

'it's very difficult to pin down the person responsible for the development of an algorithm or find out where they got it, or any of those things, and then figure out how it was designed' (Interviewee 2).

It is also difficult to track the kind of metadata that is used in some of the techniques that are employed in the SIS. The problem is that a:

'lot of the researchers do not even know where their data or their algorithms come from because there is open source stuff' (Interviewee 2).

This interviewee further said that it is concerning that there is very little transparency in the processes. Despite having people responsible for looking at ethical issues such as transparency, the landscape in which the technologies are used in the project does not provide enough opportunities for transparency. Interviewee 2 also mentioned that it could be *'more difficult to try to figure out the nature of the technology [being used] and where do all of the constituent parts come from'*. A different view, however, was given by Interviewee 3, who specifically referred to MIP and the way that it is planned to be used in the first phase. Interviewee 3 mentioned that there is transparency in the use of MIP, as a specific SIS platform, because it is a semi-automated process that guards against lack of openness in the processes by design.

Despite the concerns with transparency issues, there are mechanisms put in place to try and encourage transparency within the processes. For instance, although not always effective, there is a push towards engaging with both internal and external users of the technologies to keep them open and useable. An example of such initiatives to promote transparency is a product called Knowledge Graph that is currently being developed. The Knowledge Graph:

'will be a publicly accessible, quite transparent interface where people can look at HBP data and can perform their own research there' (Interviewee 2).

This is something that will hopefully address the digital division and transparency issues that are encountered in the use of SIS.

5.5 Mechanisms to Address Ethical Issues

As seen from the discussion above, the use of SIS in human brain research raises ethical concerns. To address these concerns, some policies govern the use of SIS, specifically related to the ethical implications of the use of SIS in the HBP. However, Interviewee 2 pointed out that there was a lack of overarching policies around the use of SIS in the HBP. To address this, the interviewee suggested that:

‘there needs to be conversation [...] because there isn't a blanket policy that will cover all of the many and varied possibilities for the HBP’.

One of the reasons for not having a blanket policy was down to the fact that the work with SIS in the HBP involves a wide range of disciplines, and therefore some people would not:

‘have the appropriate knowledge to think about how the development of specific algorithms should be governed, and they may not have the background to do a forensic examination of the tools they're using. So, it's immensely complex’.

Despite such limitations, there are specific policies on the principles and processes that govern the work in HBP, including the use of SIS. For instance, the policies cover issues related to confidentiality, informed consent, and licensing

In addition, the project has a dedicated program to provide mechanisms to ensure Responsible Research and Innovation⁴¹. This dedicated program covers the eight main components that are shown in Table 3 below.

Mechanism	Brief description
Foresight Lab	<ul style="list-style-type: none">• Investigates possible outcomes and consequences of the work undertaken by the HBP• Focuses on identifying and evaluating the future impact of new knowledge and technologies generated by the HBP using a range of methods including action research, interviews, participant observation, literature reviews, questionnaire surveys and expert workshops
Ethics Support (ES)	<ul style="list-style-type: none">• Provides administration of ethics-related issues. This includes the support of additional structures that help with ethics-related issues and structures• Manages compliance with EU research ethics principles.• Supports an external Ethics Advisory Board• Leads a cross-HBP Data Governance Working Group
Ethics Rapporteur Programme (part of ES)	<ul style="list-style-type: none">• Deepens understanding of potential ethical and social implications of research and other work in all the HBP Subprojects• Establishes communication links that help HBP achieve and maintain Responsible Research and Innovation goals

⁴¹ an approach that anticipates and assesses potential implications and societal expectations with regard to research and innovation, with the aim to foster the design of inclusive and sustainable research and innovation (European Commission, 2012)

Data Protection Officer (DPO) (part of ES)	<ul style="list-style-type: none"> • The DPO is a professional in the field of data protection and works with HBP partners to facilitate compliance with the GDPR. The role of the DPO includes consultation on data processing activities and providing advice and recommendations on compliance with applicable laws
Public Engagement	<ul style="list-style-type: none"> • Reaches out to stakeholders and the general public to discuss issues of relevance to the HBP and the public • Activities include public meetings, online consultations and stakeholder forums
Neuroethical Reflection	<ul style="list-style-type: none"> • Focusses on conceptual ethical and regulatory issues, from potential privacy threats to understanding consciousness and the meaning of human and personal identity
Ethics Advisory Board	<ul style="list-style-type: none"> • This an independent body that advises on specific ethical, regulatory issues raised by research undertaken or planned under the HBP
Data Governance Working Group	<ul style="list-style-type: none"> • It is involved with the overall management of the usability, integrity and security of data used in the HBP

Table 3: Mechanisms to deal with ethical issues in HBP

6. Conclusion

The use of SIS is making strides in human brain research geared towards understanding the complex functions of the brain and treatments of some challenging brain diseases. This case study showed how SIS is being used in one such research initiative that is taking place to understand the complex functions of the human brain. Three interviews were conducted to explore different perspectives on the use of SIS in human brain research, and which ethical issues arise from the use of SIS in human brain research.

The ethical issues that emerge from the case study resonate with issues in the literature such as privacy and confidentiality, security of personal data as well as trust and accountability by the researchers and other stakeholders, particularly when it comes to data manipulation. From the interviews, additional ethical issues were established including discrimination resulting from bias and access to the SIS and their outcomes, and transparency of the processes that are involved in human brain research due to the complexity of the technology used.

Also of interest were the different views expressed by the interviewees, who had different roles in the research, on ethical issues with the SIS. There was a difference in perspectives between those that deal with the ethical governance of the research compared with those who are responsible with the technical side of the research and therefore the implementation of the SIS. Despite the differences in perspectives across the roles, holistically there is recognition of the ethical implications that relate to the use of SIS in their research activities, and therefore the project has put in place mechanisms to safeguard against some of the consequences that could result from the use of SIS. Some of the mechanisms include dedicated ethics support, policies and guidelines as well as public engagement.

6.1 Limitations

While the HBP appears to be tackling some of the ethical issues relating to the use of SIS, some other areas need to be considered. For instance, it would be ideal if there could be an exploration of how the different views on the ethical issues across the multiple roles involved in different SIS platforms could be harmonised.

Regarding use of the SIS, despite great efforts being made in the use of different SIS across platforms, there are still limitations relating to resources and capacity that are required for the integration of the complex systems. In addition, there are differences in the progress of SIS implementation across the platforms, which sometimes affects the effectiveness of the SIS used in the project. However, this is something that will be addressed if the necessary resources are put in place.

6.2 Contribution and Implication of this Case study

While there is literature on the ethics of SIS and particularly the use of AI and Big Data in human brain research, there is still room to build on existing literature on assessing the ethical issues of implementing SIS in human brain research. To that effect, this case study contributes to knowledge around the use of SIS in human brain research. It highlights ethical issues that relate to the use of SIS in human brain research and at the same time signposts how the ethical issues could be addressed through some mechanisms used in the HBP such as Data Governance Working Groups, Neuroethical Reflection and Foresight Labs. In so doing, learning from the steps undertaken in the HBP, the case study contributes to practice by highlighting some of the practical measures that are vital in the ethical implementation of SIS.

The case study has implications for policy formulation around the ethical use of SIS in human brain research. There is little guidance on how the use of SIS can be effectively and ethically implemented in human brain research within policy frameworks. Most of the existing frameworks offer general guidelines on the ethical implementation of SIS in research, but there is a need to have guidelines that focus and directly relate to the specific issues with the

use of AI and Big data in human brain research. It is hoped that this report will encourage the assessment of ethical SIS use in current and future human brain research.

6.3 Further Research: bio-AI, see opening comments

The use of SIS in human research, as is in the case of the HBP, may lead to the next generation of SIS. At this point, it is not clear whether such new SIS, which are called bio-AI in the HBP, will raise the same or other ethical issues because it is not yet clear what their capabilities will be. While this report offers a review of some of the notable ethical issues with the use of SIS in human brain research, there may be additional foci that need to be evaluated in the future to uncover additional issues in this emergent field. It is fair to say that this case study does not answer every question on the topic, but it lays a basis for further research in the field that could enhance our understanding of ethical issues and how to address them in emergent SIS such as bio-AI.

7. References

- Alexiou, A., Theocharopoulou, G., Vlamos, P., 2013. Ethical Issues in Neuroinformatics, in: Papadopoulos, H., Andreou, A.S., Iliadis, L., Maglogiannis, I. (Eds.), *Artificial Intelligence Applications and Innovations*. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 700–705. https://doi.org/10.1007/978-3-642-41142-7_71
- Amunts, K., Ebell, C., Muller, J., Telefont, M., Knoll, A., Lippert, T., 2016. The Human Brain Project: Creating a European Research Infrastructure to Decode the Human Brain. *Neuron* 92, 574–581. <https://doi.org/10.1016/j.neuron.2016.10.046>
- Anagnostopoulos, I., Zeadally, S., Exposito, E., 2016. Handling big data: research challenges and future directions. *J. Supercomput.* 72, 1494–1516. <https://doi.org/10.1007/s11227-016-1677-z>
- Arbib, M.A., 1975. Artificial intelligence and brain theory: Unities and diversities. *Ann. Biomed. Eng.* 3, 238–274. <https://doi.org/10.1007/BF02390972>
- European Commission, 2012. Responsible Research and Innovation. Europe’s ability to respond to societal challenges. European Commission.
- Goertzel, B., Lian, R., Arel, I., de Garis, H., Chen, S., 2010. A world survey of artificial brain projects, Part II: Biologically inspired cognitive architectures. *Neurocomputing, Artificial Brains* 74, 30–49. <https://doi.org/10.1016/j.neucom.2010.08.012>
- Hassabis, D., Kumaran, D., Summerfield, C., Botvinick, M., 2017. Neuroscience-Inspired Artificial Intelligence. *Neuron* 95, 245–258. <https://doi.org/10.1016/j.neuron.2017.06.011>
- Huerta, M.F., Koslow, S.H., Leshner, A.I., 1993. The human brain project: an international resource. *Trends Neurosci.* 16, 436–438. [https://doi.org/10.1016/0166-2236\(93\)90069-X](https://doi.org/10.1016/0166-2236(93)90069-X)
- Human Brain Project, 2018. Human Brain Project: Welcome to the Human Brain Project [WWW Document]. URL <https://www.humanbrainproject.eu/en/>

- INCF, 2018. Why neuroinformatics? [WWW Document]. URL <https://www.incf.org/about/why-neuroinformatics> (accessed 9.10.18).
- LeCun, Y., Bengio, Y., Hinton, G., 2015. Deep learning. *Nature* 521, 436–444.
<https://doi.org/10.1038/nature14539>
- Prieto, A., Prieto, B., Ortigosa, E.M., Ros, E., Pelayo, F., Ortega, J., Rojas, I., 2016. Neural networks: An overview of early research, current frameworks and new challenges. *Neurocomputing* 214, 242–268. <https://doi.org/10.1016/j.neucom.2016.06.014>
- Reger, B.D., Fleming, K.M., Sanguineti, V., Alford, S., Mussa-Ivaldi, F.A., 2000. Connecting Brains to Robots: An Artificial Body for Studying the Computational Properties of Neural Tissues. *Artif. Life* 6, 307–324. <https://doi.org/10.1162/106454600300103656>
- Rommelfanger, K.S., Jeong, S.-J., Ema, A., Fukushima, T., Kasai, K., Ramos, K.M., Salles, A., Singh, I., Amadio, J., Bi, G.-Q., Boshears, P.F., Carter, A., Devor, A., Doya, K., Garden, H., Illes, J., Johnson, L.S.M., Jorgenson, L., Jun, B.-O., Lee, I., Michie, P., Miyakawa, T., Nakazawa, E., Sakura, O., Sarkissian, H., Sullivan, L.S., Uh, S., Winickoff, D., Wolpe, P.R., Wu, K.C.-C., Yasamura, A., Zheng, J.C., 2018. Neuroethics Questions to Guide Ethical Research in the International Brain Initiatives. *Neuron* 100, 19–36.
<https://doi.org/10.1016/j.neuron.2018.09.021>
- Shapshak, P., 2018. Artificial Intelligence and brain. *Bioinformation* 14, 38–41.
<https://doi.org/10.6026/97320630014038>
- Shepherd, G.M., Mirsky, J.S., Healy, M.D., Singer, M.S., Skoufos, E., Hines, M.S., Nadkarni, P., Miller, P.L., 1998. The Human Brain Project: neuroinformatics tools for integrating, searching and modeling multidisciplinary neuroscience data. *Trends Neurosci.* 21, 460–468.
- Stahl, B.C., Wright, D., 2018. Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation. *IEEE Secur. Priv.* 16, 26–33.
<https://doi.org/10.1109/MSP.2018.2701164>

CS06 – Insurance



Case Study: Insurance, Smart Information Systems and Ethics



**This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641**



Document Control

Deliverable	Deliverable 1.1.: Case Studies
WP/Task Related	WP 1: Representation and Visualisation
Delivery Date	Date Deliverable Due 31/1/2019
Dissemination Level	Public
Lead Partner	University of Twente
Contributors	Natalija Kancevičienė, EUREC
Reviewers	Kevin Macnish, Mark Ryan
Abstract	This report provides an overview of the current implementation of SIS in the insurance industry, also identifies the positive and negative aspects of using SIS in the insurance industry, including ethical issues which could arise while using SIS in this area. Two companies working in the industry of health insurance are analysed in this report: a German health insurance company (Organisation Y), and a business intelligence centre for healthcare insurers (Organisation X). Further specific ethical issues that arise when using SIS technologies in Organisation Y and Organisation X are critically evaluated. Finally, conclusions are drawn on the case study and areas for improvement are suggested.
Key Words	Insurance, smart information systems, ethics, Big Data

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes
1.1	20/11/2018	Natalija Kancevičienė	Kevin Macnish, Mark Ryan	
1.2	27/11/2018	Natalija Kancevičienė	Kevin Macnish, Mark Ryan	
1.3	09/01/2018	Natalija Kancevičienė		

Contents

Executive Summary	171
Insurance SIS and Ethics: A Case Study	173
1. The Current Use of SIS in Insurance	174
2. Ethical Issues of Using SIS in Insurance	177
2.1. Accessibility of Data and Data Governance	178
2.2. Security and Privacy	178
2.3. Bias and Reliability	179
2.4. Job losses	179
2.5. Discrimination	180
2.6. Transparency	180
3. Organisation X: The Case of an Insurance Company Using SIS	180
3.1. Description of Organisation X	181
3.2. Description and Aims of Smart Technologies Being Used in Organisation X	181
3.3. The Effectiveness of Using Smart Information Systems for Organisation X	182
3.4. The Effects on Stakeholders	182
4. Organisations Y: The Case of an Insurance Intelligence Centre Using SIS	183
4.1. Description of Organisation Y	184
4.2. Description and Aims of Smart Technologies Being Used in Organisation Y	184
4.3. The Effectiveness for Using SIS for Organisation Y	184
4.4. The Effects on Stakeholders	185
5. Ethical Issues from SIS Technology	185
5.1. Accuracy of Data and Recommendations	186
5.2. Employment	187
5.3. Responsibility	187
5.4. Ownership of Data	187
5.5. Transparency	188
5.6. Trust	189
5.7. Informed Consent	189
5.8. Use of Personal Data and Security	189
6. Conclusion	190
6.1. Limitations	191
6.2. Contribution to Knowledge	192

6.3. Implications of This Report	193
6.4. Further Research	193
7. References	193

Executive Summary

Smart information systems (Artificial intelligence and Big Data) are used in the insurance industry most often to improve customer service, strategic planning and corporate development, marketing and sales, tracking of market sales and insurance product development. In this case study I looked at how two organisations in the insurance industry (Organisation X and Organisation Y) are using smart information systems in their practice. Organisation X is one of Germany's largest private health insurance companies and it uses smart information systems for fraud detection. Organisation Y is the business intelligence centre for healthcare insurers, providers and the public. It uses smart information systems for analysis of the insurance data given most often by insurance companies to make information products (e. g. predictive models), which later help the insurance companies and health care institutions to improve their work, increase the efficiency of administrative processes in healthcare, etc.

In recent years insurance sector has invested the most comparing with other sectors into implementation of smart information systems making it already one of the top industries, by average, investing in smart technologies. More than half of insurance CEOs believe that artificial intelligence and Big Data will transform their workplace, improve productivity, customer experience and their work-life balance. Moreover they believe that smart information systems implemented in their workplace will make their jobs simpler and result in a net gain in jobs within their companies. However, the use of smart information systems in insurance sector may also create a number of ethical and practical concerns. For example, concerns over security and privacy of sensitive information, which are increasing year by year because of several trends, such as wireless networking, health and personal information exchange, and cloud computing. As a result, artificial intelligence may make many false assumptions in the insurance sector which could end up being discriminatory (e.g. making insurance more expensive for minorities), and even harmful to the insured persons (e. g. when healthcare isn't affordable for the person who needs it). The lack of availability of artificial intelligence skilled labour is also a huge challenge for companies in the insurance sector – if not addressed this issue could result as massive job loss. Also, there are limited strategies to uncover questions regarding transparency when using smart information systems – that is a possibility for users or staff to clearly understand when, why and how the decisions by artificial intelligence are made, when and why their personal information is used and for what purposes. There are many recommendations for the proper use of smart information systems in the insurance industry but it currently lacks specific regulations.

In this case study, Organisation X and Organisation Y to address the mentioned ethical issues are working according to the national and European data protection regulation and cooperate with data protection officers. Moreover Organisation Y also has organisational regulation for proper use of the software and an external auditor who audits

processes to see if everything works according to the legislation once every year. Also in both organisations all stakeholders (e. g. customers, insurance companies) have the ability to share their concerns about lack of transparency, data protection issues, etc. with the staff of Organisation X or Organisation Y. Organisation X has a board of directors which can give their feedback about the processes in the company (including the software), and a quality control mechanism to ensure that everything is working as it should. Organisation Y gets feedback from insurance companies in group discussions. They also send requests to health insurance companies every month to get their consent for using their insurance data for other purposes, for example meeting requests from universities or institutes to use the data for research.

The interviews have shown that when using smart information systems in the insurance sector some ethical issues identified in the literature are not emphasized as significant or not identified as issues at all in the interviews (such as bias, reliability, discrimination, data governance, security and privacy, job losses). However, some ethical issues were not mentioned as significant in the literature but were identified as very important during the interviews (e.g. trust, informed consent, responsibility). Transparency and accessibility of data as ethical issues appeared to be important in both literature and practice.

Insurance SIS and Ethics: A Case Study

Thousands of claims, customer queries and large amounts of diverse data make the insurance industry a natural use case for smart information systems (SIS). A study from 2015 conducted by Tata Consultancy Services reported that the insurance sector in 2015 invested in artificial intelligence far more than other industries: \$124 million dollars, compared with an average by other industries of \$95 million (consumer packaged goods), \$94 million (high tech), \$90 million (telecommunications) (Tata Consultancy Services Ltd (TCS), 2017).

From customer service to claims processing, AI is frequently cited as a disruptive force⁴² in the insurance sector (Expert System, 2018). 80-85% of insurance companies use SIS in 2018, from scanning in text from documents, to determining fraud, identifying risks or in preventative medicine. There are already many start-ups in the insurance sector (such as Shift Technology, Lemonade, Clover, ABle) which use SIS in many areas including claims processing, fraud detection, risk management, marketing, etc. All the insurance companies surveyed plan to use SIS in their processes by 2020. (Tata Consultancy Services, 2017; Tata Consultancy Services Ltd (TCS), 2017; Dutt, 2018)

There is moreover a consensus among industry experts that AI is going to be a key driver in making insurance products “smarter” in the coming 2-3 years (Bharadwaj, 2018; Zagorin, 2018). Most insurance executives already understand that SIS will change the insurance industry – 79 per cent of insurance executives believe that it will revolutionize the way insurers gain information and interact with their customers (Zagorin, 2018). Despite all the financial aspects and the range of possible issues raised, there is a great possibility that in the near future insurance companies will be required to adopt SIS or risk being outperformed by other insurance companies (Accenture, 2018).

This literature review and the background research draw on information from three studies conducted by private companies on the use of SIS in the insurance sector, in which the benefits of SIS were also highlighted:

1. Accenture (2018). *Future Workforce Survey – Insurance. Realizing the Full Value of AI*;
2. Deloitte Digital (2017). *From mystery to mastery: Unlocking the business value of Artificial Intelligence in the insurance industry*;
3. Tata Consultancy Services Ltd (TCS) (2017). *Getting Smarter by the Sector: How 13 Global Industries Use Artificial Intelligence*).

Section 1 of this report provides an overview of the current implementation of SIS in the insurance industry. In Section 2 the positive and negative aspects of using SIS in the insurance industry are identified, including ethical issues which could arise while using SIS in

⁴² A force that does not rely on incremental changes but rather transforms a sector quickly.

this area. In Sections 3 and 4, two companies working in the industry of health insurance are analysed: a German health insurance company (Organisation Y), and a business intelligence centre for healthcare insurers (Organisation X). Section 5 will critically evaluate specific ethical issues that arise when using SIS technologies in Organisation Y and Organisation X, also those questions regarding data governance when using SIS and the use of SIS in the insurance industry. Finally, Section 6 draws conclusions on the case study and suggests areas for improvement.

1. The Current Use of SIS in Insurance

There are many types of data that are analysed in insurance data analytics. These include personal information such as place of residence, (location, marital or family status, education, occupation, income level is also gathered (Foggan and Panagakos, 2018) other customer data (concerning their driving habits, etc.) (Bharadwaj, 2018; Sennaar, 2018), information gathered by Internet of Things (IoT) sensors (Foggan and Panagakos, 2018; Koh and Tan, 2018), for homes, sensors for vehicles (Bharadwaj, 2018; Zagorin, 2018) and vehicle maintenance history (Zagorin, 2018). Moreover healthcare data and records (Foggan and Panagakos, 2018; Koh and Tan, 2018, Zagorin, 2018) of insured persons (especially in health insurance) is collected and processed by insurance and related companies. Insurance claims history (Marr, 2018; Koh and Tan, 2018) and incident-related information (Marr, 2018) is checked to prevent fraud or to decide about premiums. It is also possible to collect open source content which is free to use without permission (Deloitte Digital, 2017) and social data (Bharadwaj, 2018; Deloitte Digital, 2017) related to insured persons. Information is collected from a variety of sources in insurance, such as social networks, including Facebook, LinkedIn, Instagram, etc. (Bharadwaj, 2018; Zagorin, 2018), and other public sources, e. g. registries, statistical data (Dutt, 2018). Companies' call logs (Deloitte Digital, 2017) are also often checked to analyse possible scenarios of claims management and monitor the quality of services.

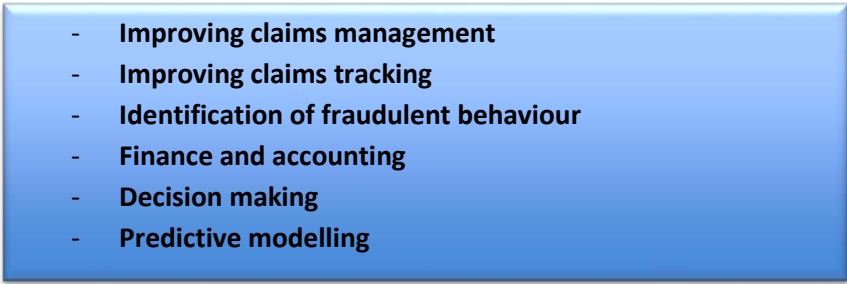
All gathered data is mostly applied to those areas of the insurance industry which can help to improve services and bring profit, such as:

Figure 1. Areas of data use in the insurance industry.



This data also play a vital role in helping to save many of the insurance companies money by:

Figure 2. Possible ways to save money with SIS in the insurance industry.

- 
- **Improving claims management**
 - **Improving claims tracking**
 - **Identification of fraudulent behaviour**
 - **Finance and accounting**
 - **Decision making**
 - **Predictive modelling**

Faster analysis of large volumes of data and faster and customized claims settlement is now possible in the insurance industry, as enabling SIS self-service, helps improve customer experience and use of on-demand insurance (Zagorin, 2018; Foggan and Panagakos, 2018; Deloitte Digital, 2017; Bharadwaj, 2018). Personalized interactions with customers and personalized insurance product development are now possible (Zagorin, 2018; Koh and Tan, 2018; Bharadwaj, 2018; Accenture, 2018). Moreover, SIS also helps insurance companies to get the latest knowledge in real time and identify new business opportunities (Bharadwaj, 2018; Deloitte Digital, 2017).

There are also benefits to the staff of insurance companies, because SIS improves productivity (Accenture, 2018), reduces resources needed (which decreases costs) (Bharadwaj, 2018), makes the job simpler (Accenture, 2018; Deloitte Digital, 2017), gives assistance in making decisions (Accenture, 2018; Koh and Tan, 2018) and even expands career prospects for workers (Accenture, 2018).

Smart information systems are and will be very important for insurance companies in the future. However in 2016 only 1.33 % of insurance companies had invested in AI (Deloitte Digital, 2017). By 2018, 49% of insurance companies' CEOs are looking at strategic alliances or joint ventures with insurance technology (InsurTech) companies to speed up their alignment with the digital marketplace. The expectations are high.

For example a report on two surveys conducted by consultancy Accenture P.L.C. in 11 countries in 2017 states that artificial intelligence is likely to transform the world of business and, "when synthesized with human ingenuity across the enterprise, will achieve exponentially more" (Accenture, 2018). According to information from the report, more than half of insurance CEOs believe that artificial intelligence and Big Data will transform their workplace, improve productivity, result in a net gain in jobs within their company, make their jobs simpler and improve their work-life balance (Accenture, 2018). Another big survey conducted in 2015 states that 100% of insurance companies plan to use cognitive

technologies by 2020. Representatives of the insurance industry claim to be so optimistic about using SIS in the insurance industry because, they say, when they started to use SIS they reduced their losses by being able to identify fraudulent claims more easily (Bharadwaj, 2018; Zagorin, 2018; Foggan and Panagakos, 2018; Koh and Tan, 2018; Deloitte Digital, 2017) and improve predictive modelling (Foggan and Panagakos, 2018; Koh and Tan, 2018). It is also claimed that the insurance industry is already one of top industries, by average, investing in smart information systems (Tata Consultancy Services Ltd (TCS).

There are many start-ups in which SIS are being used in the insurance sector worldwide. Some examples of these start-ups are described below.

Shift Technology uses AI called Force™ for fraudulent claims identification. Shift Technology's official website claims that Force™ has already analysed over 100 million claims for fraud. It claims that Force™ goes beyond simple risk provision by furnishing clear, actionable insights on which indicators make the claim suspect (Shift Technology, 2018). Shift Technology claims to have fused the analytic powers of machines with industry expertise to reproduce the deductive reasoning of claims handlers to create Luke™ for claims handling. From the filing of a claim to the policyholder payout, Shift says that Luke™ will help at every step, reducing end-to-end handling time from weeks to minutes (Shift Technology, 2018).

Lemonade is an app for claims management, available for Mac and Android. It currently offers renters, condo, and homeowners' insurance in some states in the USA. While using Lemonade, claims are handled by artificial intelligence and humans. If the claim is instantly approved, Lemonade's AI pays in 3 seconds. Otherwise, AI hands over the claim to the team of humans to handle (Lemonade Insurance Company, 2018).

Clover is a health insurance start-up that leverages AI by using data and software to build clinical profiles of people. This app uses AI to identify gaps in care and fill them with visits and a free choice of doctor to avoid costly hospital stays (Deloitte Digital, 2017). Clover's official website claims that it also helps to find the right doctor or pharmacy, gives assistance in scheduling appointments and arranging transportation, gives medications reminders, offers 24/7 doctor visits by phone, video or mobile app, and gives access to a mail order pharmacy with 100-day refills (Clover Health, 2018).

Fabric is a life assurance start-up that is using AI to generate quotes for accidental death claims. It is claimed that simplified processes enable a life assurance sign-up process in just two minutes (Deloitte Digital, 2017).

GetSafe is an InsurTech start-up that uses AI to advise customers on which insurance policies to purchase by collecting relevant information (Deloitte Digital, 2017). GetSafe also proactively engages with clients to offer preventive health measures by setting reminders when it is time to have routine care, or to set an appointment with a health specialist, etc. (Wiens, 2018).

Trov is an on-demand property insurance start-up in which an AI chatbot⁴³ handles claims. Insurance can start immediately via an app to cover damage, loss, and theft. When using this app, customers can swipe insurance on their valuables on or off. **Error! Bookmark not defined.** The customer also has the option to easily organise important information about the things they own and back this up to the cloud, so it is accessible when needed (Trov, Inc., 2018).

Progressive offers the Snapshot[®] program, which personalizes driver's insurance premium rate based on their actual driving, known as usage-based insurance. There are other pricing factors, and drivers' rates may increase with high-risk driving (Progressive Casualty Insurance Company, 2018). Progressive is also using AI to identify business opportunities in the auto insurance space. The company is using machine learning to interpret driver data to track market trends and identify business opportunities (Bharadwaj, 2018).

All these mentioned examples show, that there are loads of various cognitive technologies already being used in the insurance area and it strongly supports the point that in the near future smart information systems in insurance industry will be a necessity to stay competitive. That is why there is a great need to intensively work to identify possible ethical issues when using smart information systems and find effective ways to prevent them.

2. Ethical Issues of Using SIS in Insurance

Despite the claims to business and consumer benefit SIS raises a range of ethical issues. The foundation upon which smart information systems is built is the harvesting of personal information from millions of people, and the use of that information to make decisions affecting millions more, which entails new concerns and risks, and ultimately may increase the number of issues which insurers must address (Foggan and Panagakos, 2018).

Information on the use of smart information systems in the insurance industry and the ethical issues arising therefrom is sparse. Most research is done on implementing smart information systems in insurance, and the benefits of that, but little information is available about ethical issues when using SIS, or its possible drawbacks. The following sections describe ethical issues identified in the literature.

Moreover, there are already many recommendations developed to address ethical issues when using smart information systems in insurance, but the problem is that it is not known how to implement those recommendations into policy.

⁴³ A computer program or AI, which can conduct a conversation.

Figure 3. Ethical issues in the literature – smart information systems and insurance.



2.1. Accessibility of Data and Data Governance

Insurance companies which are using smart information systems rely on data. Data make smart information systems a key competitive differentiator in the future of intelligent insurance (Deloitte Digital, 2017).

Within the organizational limits required by regulation and security, data are essential for insurance companies for training and machine learning (Dutt, 2018). Often there are problems in collecting data. The main limitation is accessibility of the data, because data often exists in different settings and systems, such as administrations, clinics, laboratories, registers, public and private companies (Koh and Tan, 2018).

There are many questions regarding data governance when using smart information systems and the use of SIS in the insurance industry currently lacks specific regulations, except for the General Data Protection Regulation (GDPR) and other legal documents, which are being used in all industries across Europe. Moreover some additional questions need to be answered to clarify the situation. For example, when should a decision by an artificial intelligence be trusted? Is an AI to be used as a final decision maker or as an adviser to recommend certain decisions? How do you match outcomes to the decision made by artificial intelligence, and what is the feedback process to make changes to the artificial intelligence if errors are discovered? Only by creating a controlled environment for the use of artificial intelligence, is it possible for the technology to benefit as many people as possible and minimize its dangers (Dutt, 2018).

2.2. Security and Privacy

Adoption of smart information systems in the insurance sector raises many barriers and challenges. Concerns over security and privacy of sensitive information are increasing year by year because of several trends, such as wireless networking, health and personal information exchange, and cloud computing (Abouelmehdi et al., 2018).

When talking about security, authentication is very important. Authentication is understood as the act of establishing or confirming that claims made by or about a subject are true. It serves a vital function within any insurance organisation in many areas, such as

securing access to corporate networks, protecting the identities of other users, and ensuring that a user is who he or she claims to be (Abouelmehdi et al., 2018).

The most obvious issues when using smart information systems concern privacy. For example, if AI is able to determine that someone has a certain disorder or disease by correlating public pieces of information gleaned from social networks or public sources, an argument could be made that this constitutes a violation of privacy rights or is, at the very least, ethically questionable (Dutt, 2018). AI uses not only public information about the client but also their personal information which, according to the General Data Protection Regulation, is considered to be more sensitive. As a result the ethical harm is even more serious in this situation.

2.3. Bias and Reliability

Data may be missing, corrupted, inconsistent, or non-standardized (such as pieces of information recorded in different formats in different data sources), and lack a standard vocabulary. Data problems in healthcare are often perceived to be the result of the volume, complexity and heterogeneity of the data, their poor mathematical characterisation, and their non-canonical form (Koh and Tan, 2018). When data are not statistically sound, they reduce their efficacy for training (Dutt, 2018). As a result, artificial intelligence may make many false assumptions in the insurance sector which could end up being discriminatory (e.g. making insurance more expensive for minorities).

The validity of the results of AI-based decision making in the insurance sector may also be questioned. The familiar aphorism that correlation is not causation (meaning that not always statistical probability reflects a true cause) holds true here as elsewhere. Moreover, some characteristics that correlate with increased risk or suspicion of fraud might be challenged as discriminatory to the extent there is no demonstrable causal connection between the characteristic and the risk of suspicion (Bharadwaj, 2018).

2.4. Job losses

Although artificial intelligence and smart information systems have been promised as problem-solvers, they have also sparked concerns about job losses. Japanese insurer Fukuoka Mutual Life Insurance announced that it would replace more than 30 employees with an artificial intelligence system (Newton Media, 2018). Mariana Dumont, head of new projects at Insurance Nexus, states: “in conversations I’m having with insurance executives, I’ve noticed that we are all very excited about where AI is headed in the insurance industry, but there’s a lot of uncertainty, we don’t know how it will change the core business model, and peoples’ jobs.” (Bharadwaj, 2018)

The managers of insurance companies surveyed felt AI could automate on average 10% jobs in their own departments in 2016. Looking further ahead, they anticipated that an

average of 14% could be cut in 2020 in functions using AI, and 18 % of jobs could be automated by 2025 (Tata Consultancy Services Ltd (TCS), 2017).

The lack of availability of artificial intelligence skilled labour is also a huge challenge for companies in the insurance sector. Any artificial intelligence technology integration would need technically skilled professionals in an organization to train these artificial intelligence systems (Bharadwaj, 2018). However, the skills requisite for training artificial intelligence will become redundant once the artificial intelligence is fully functional, to be replaced by a need for skills in maintaining artificial intelligence and relevant hardware performance.

2.5. Discrimination

As smart information systems become more sophisticated, ethical issues (such as discrimination) also start to emerge. The predictive modelling capacities of artificial intelligence systems constitute a natural “fit” to the assessment of risk inherent in the processes of insurance ratemaking and pricing. Advanced predictive modelling can generate “red flags” during the claim intake process, which enables suspect claims to be routed for investigation while proper claims proceed to payment. If an artificial intelligence is used to prevent some people from receiving health insurance (for example, by determining that someone has a certain disorder or disease by correlating public pieces of information gleaned from social networks or other public sources) then the reasons should be clearly understood to prevent implicit and harmful biases (Dutt, 2018). These developments could result in a charge of unfair discrimination in insurance which might also be levelled against practices which impact people based upon characteristics such as income level, place of residence, occupation, education, marital or family status (Foggan and Panagakos, 2018).

2.6. Transparency

Transparency means a possibility for users or staff to clearly understand when, why and how the decisions by artificial intelligence are made, when and why their personal information is used and for what purposes. Currently there are limited strategies to uncover all those questions. Even determining which set of variables are the most relevant for the artificial intelligence model is not always easy (Dutt, 2018), because artificial intelligence chooses those completely by itself in accordance with its experience. Although the customer has a legal right to be informed about the use of this personal data. That is why it is very important what methods insurance professionals will use to be able to respond fully to customer requests for explanation of the reasoning that underlies those determinations, given the mystery that cloaks the algorithms by which cognitive systems produce their results (Bharadwaj, 2018).

3. Organisation X: The Case of an Insurance Company Using SIS

This section will focus on Organisation X, a company that implements and uses smart information systems technology within the insurance sector (the organisation has asked that it and the name of the interviewee be anonymised). An interview was conducted with Interviewee X, the head of operating services in the company, who is responsible for underwriting, contracts, and management of claims, and who reports directly to the board of the organisation. Interviewee X is not involved much in working with smart information systems used by Organisation X, but Interviewee's X interest in this is the outcome of using SIS. The interview raised Interviewee's X interactions with smart information systems in the company, possible issues associated with ethics, technological drawbacks and use of data (accuracy of data and recommendations, employment, responsibility, ownership of data, transparency, trust, informed consent, use of personal data and security), and how the company addresses these issues. The interview was conducted by Natalija Kancevičienė (a research assistant in European Network of Research Ethics Committees (EUREC)) in 2018 via telephone, and transcribed and evaluated also by Natalija Kancevičienė using the qualitative analytics software tool NVIVO to categorise, define, and evaluate the content of the interview.

Table 1. *Organisation's X interview.*

Duration: 22 minutes

Interviewee Interviewee X

Reference in Case Study Interviewee X

Role in Organisation Head of operating services

3.1. Description of Organisation X

Organisation X is located in the service and insurance industry. It is one of Germany's largest private health insurance companies, with more than 2 million members. The company serves approximately 5 million insured people by suggesting them most suitable health insurance according to their health information. Organisation X is a for profit organisation and an innovative health insurance company, which uses SIS for identifying fraudulent claims. As one of Organisation X's directors explained, the company wants to make sure that their members always have access to the very best procedures, when it comes to detecting and treating illnesses.

3.2. Description and Aims of Smart Technologies Being Used in Organisation X

Organisation X is using one smart information system at present. This is a customised, self-programmed software for fraud detection in private health insurance. The system stands alone, and is not implemented or supported by other systems in Organisation X. Interviewee X stated that the system is able to identify, as they refer, abnormal behaviour (for example, when a person gets medicine from a lot of different pharmacies instead of going to the pharmacy nearest to home). According to Interviewee X, this system makes it easier and faster to identify fraudulent claims.

3.3. The Effectiveness of Using Smart Information Systems for Organisation X

In fraud detection Organisation X no longer depends only on people paying attention during the claims management process.

“In fraud detection we any longer depend only on people or colleagues paying attention during the claim process. Now we have a software, which selects cases with a possibility of fraudulence, so we can focus on these cases only” (Interviewee X, 2018)

The software selects cases with possibility of fraudulent activity so employees need to focus only on those cases. Organisation X started using the software in one field in the claims management concerning receipts of medication. Two facts serve as a motivation to expand the implementation of this system in the contracts department: the fact that the system works very well and Organisation X doesn't have any problems using it, and also that it simplifies the work of employees in the claims management and fraud detection.

Just one practical limitation was identified: the possibility of false positives, such as identifying strange or unusual behaviour as fraudulent even if it is not (for example, when a person gets the medicine from a lot of different pharmacies instead of from the pharmacy nearest to home). No other limitations of the used software have been identified yet.

“If a person gives us prescriptions for medicine for a claim and the person gets the medicine from a lot of different pharmacies, this could be identified as an abnormal behaviour. In these claims the possibility of fraud is higher rather than in situations when people buy medicine in a pharmacy near their home. Of course, there is a possibility that a person who needs medicine travels all over Germany” (Interviewee X, 2018)

Organisation X is working with the software according to the data protection regulation of Germany and of the European Union (General Data Protection Regulation (GDPR)) and Organisation X closely cooperates with the in-house data protection officer when using the technology. Moreover there is a process of quality control for using the software. But there is no organisational policy for using the software for fraud detection.

3.4. The Effects on Stakeholders

Interviewee X claims that there is no special impact on stakeholders from using smart information systems. Interviewee X claims, that more or less they are aware of smart information systems use in the organization. The main stakeholders in Organisation X are users, in-house data protection officer, the board, and decision makers.

Personal data of the users is used for the claims management process. For example, clients send personal information, what kind of medicine they have been prescribed, and the location of the pharmacy. All this information is used. There is some non-financial cost for users in terms of privacy and reduced understanding of the system because they don't know why smart technology makes the decisions it does.

The in-house data protection officer needs to make sure that using smart information system is complying with the general data protection regulation. The board of Organisation X needs sometimes to inform the media that Organisation X is using smart information system. Smart technology also assists the decision makers on making decisions about whether a claim is fraudulent and therefore whether it should be paid.

It is important that data protection officer, Organisation's X board of directors and other decision makers are able to provide their comments and opinions regarding smart information systems to the personnel of Organisation X.

4. Organisations Y: The Case of an Insurance Intelligence Centre Using SIS

This section will focus on Organisation Y: all national healthcare insurance companies share their payments data to health care organisations with this organisation (the organisation has asked that it and the name of the interviewee be anonymised). An interview was conducted with Interviewee Y, who is not involved much in working with smart information systems in the organisation, although Interviewee Y has a broad understanding of the situation surrounding smart technologies. Interviewee Y is responsible for information security, insurance programs, and regulation. During the interview, Interviewees Y's interactions with smart information systems in the company, possible issues associated with ethics, technological drawbacks and using of data (accuracy of data and recommendations, employment, responsibility, ownership of data, transparency, trust, informed consent, use of personal data and security), and how the company addresses these issues were all discussed. The interview was conducted by by Natalija Kancevičienė (a research assistant in European Network of Research Ethics Committees (EUREC)) in 2018 via telephone. The interview was transcribed and evaluated also by Natalija Kancevičienė (EUREC) using qualitative analytics software tool NVIVO to categorise, define, and evaluate the content of the interview.

Table 2. *Organisation's Y interview.*

Duration: 23 minutes	
Interviewee	Interviewee Y
Reference in Case Study	Interviewee Y
Role in Organisation	Responsible for information security, insurance programs, and regulation

4.1. Description of Organisation Y

Organisation Y is a private organisation in the health insurance industry. It is the business intelligence centre for healthcare insurers, providers and the public. Organisation Y gets insurance data from the insurance companies and analyses it to develop relevant information for those companies and for research institutions, which they call “information products” (e. g. predictive models; information, helping to improve administrative processes in healthcare). It also provides public information, for instance on its website. Cities, individuals and research projects can make requests for analyses.

4.2. Description and Aims of Smart Technologies Being Used in Organisation Y

Organisation Y has long used software it designed itself for analysis of the insurance data given by insurance companies and insured persons. Organisation Y provides insurance companies or other interested institutions (universities, research institutes) with information products (they depend on what data analysis the health insurer has asked for) which they can use in research or developing policies in health insurance. Organisation Y creates insights in healthcare consumption (volume, cost and quality) based on data-analytics. Among its clients are hospitals, general practitioners, health insurers, the government, universities and other research institutes. The software helps Organisation Y to achieve the goals they agree with the aforementioned organisations.

4.3. The Effectiveness for Using SIS for Organisation Y

Organisation Y also has organisational regulation for proper use of the software. Moreover Organisation Y has an external auditor who audits processes to see if everything works according to the legislation once every year. That is why Organisation Y has been using the software for research for a few years and no significant technological problems have been identified.

The software creates insights in healthcare consumption (volume, cost and quality) based on data-analytics and helps Organisation Y to make qualitative information products. The greatest but not very significant limitation identified by the Interviewee Y is the

limitation of data collection. Organisation Y uses only that data which is allowed by the health insurer. The interviewee stated that

“All the things we do, we do in consent of the health insurer” (Interviewee Y, 2018)

Although, if any other problems arise (technological, ethical, social, etc.), health insurance companies’ representatives or the representatives of universities and other research institutes which order information products have a possibility to share their concerns with the responsible staff of Organisation Y. Organisation Y works for those companies by making information products based on the data the insurance companies give them, so it is very interested in keeping the used systems working smoothly.

4.4. The Effects on Stakeholders

In Organisation Y the stakeholders are mostly health insurance companies, health professionals and patients. Although sometimes universities and other research institutes ask to have an analysis of insurance data. According to Interviewee Y there is a direct and indirect impact made on the stakeholders: the insurance companies, research institutes are those interested stakeholders which get the information products about how the administrative processes in healthcare should be improved, and others (patients, health professionals, etc.) are those indirectly effected by the improved processes.

Health insurance companies are the main clients of Organisation Y. They provide insurance data for Organisation Y, and Organisation Y, after the data analysis, makes information products for them to use in policy making and research. Organisation Y has an obligation always to inform them and ask their permission about using the insurance data that they have provided. Insurance companies have the ability to provide suggestions and comments about the software which is used for analysing the data. Organisation Y has held group discussions with the participation of health insurance companies to get their opinions and insights about the data analysis.

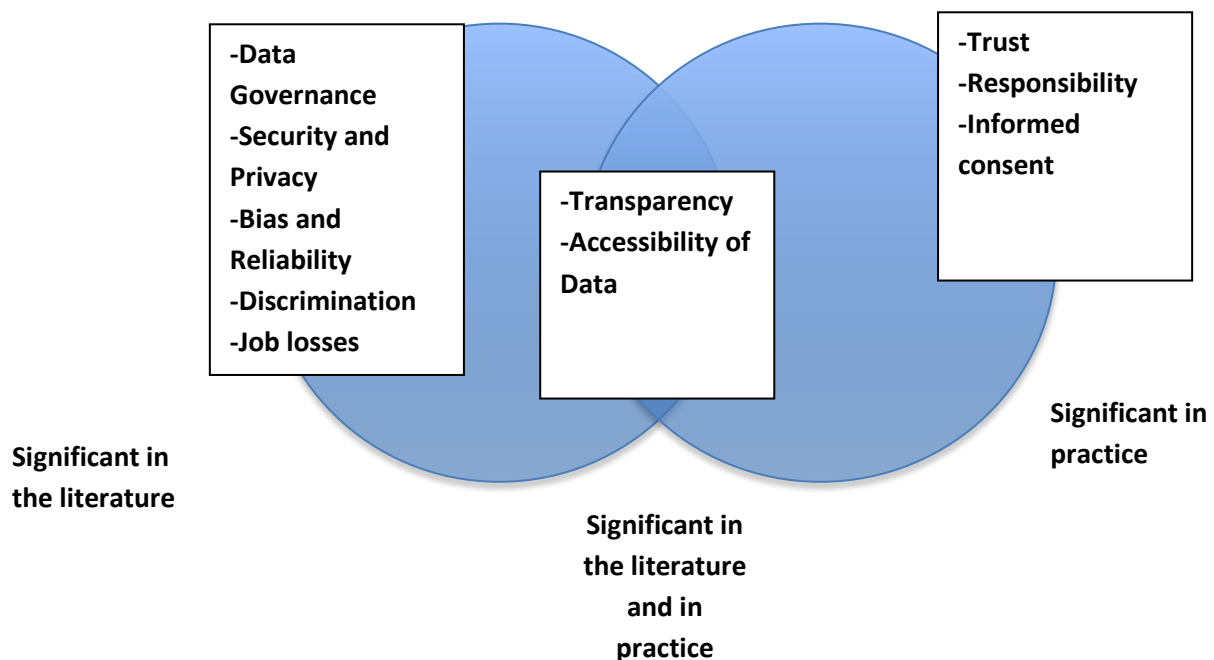
Insurance data (including personal data) of the patients is used for analysis in Organisation Y. They provide their data to the insurance companies, and they must be informed about the possibility of their data being used for analysis. If patients want to get information as to what is done with their data they can read the privacy statements of their health insurer. The policy of Organisation Y is in line with the privacy statements of the health insurance companies.

Universities and other research institutes sometimes approach Organisation Y to make insurance data analysis with data from insurance companies. These situations are difficult because the universities don’t provide any data themselves, so Organisation Y needs to ask insurance companies to let them use their data.

5. Ethical Issues from SIS Technology

There were a number of ethical issues identified during the interviews as a result of using smart technologies in the interviewed organisations. These are similar to those identified in the literature review, but not identical. Some ethical issues identified in the literature are not emphasized as significant or not identified as issues at all in the interviews (such as bias, reliability, discrimination, data governance, security and privacy, job losses). However, some ethical issues were not mentioned as significant in the literature but were identified as very important during the interviews (e.g. trust, informed consent, responsibility). Also transparency and accessibility of data as ethical issues appeared to be important in both literature and practice.

Figure 4. Correlation between ethical issues: literature vs. practice.



5.1. Accuracy of Data and Recommendations

It is important to state that there is a strong link between accuracy of data and accuracy of recommendations. Organisation Y provides insurance companies or other interested institutions (universities, institutes) with information products which they can use in research or developing policies in health insurance. The recommendations of Organisation Y are based on the data given by insurance companies. As the interviewee stated, the accuracy of data provided reflects the accuracy of recommendations.

Organisation X is using qualitative medical data (e.g. medicine used, location of pharmacy) and quantitative medical data (information from the receipts for medication) for

the identification of fraudulent claims. Also it gets personal information about the client (the insured person). They get data from their clients (the insured persons) for claim process and enter it into the software. Interviewee X explained that when data is retrieved from an insured person, accuracy is very important. A human mistake could mean that the claim is incorrectly identified as fraudulent.

Another issue identified by Organisation X and related to data is accuracy of recommendations, e. g. when the software in some situations identifies uncommon behaviour as abnormal. For example, if a person travels all over the country and gets medicine from different pharmacies, this could be identified as abnormal and the claim incorrectly interpreted as fraudulent.

5.2. Employment

When using software for fraud detection, Interviewee X said that they do not need to depend only on colleagues' opinions, because the software selects cases with a possibility of fraud and people just need to focus on those cases, instead of inspecting them all. Moreover, Organisation X is planning to expand the use of this software and implement it in the contracts department. This means that in the future fewer people will be needed for identification of fraudulent claims and contracts processing.

5.3. Responsibility

Responsibility is understood quite differently between Organisation X and Organisation Y, but it is because of the differences in their functions. Organisation X is working with data received directly from insured persons, so they are responsible for it. That is quite clear for them. They are working according to all national and European data protection regulation laws, and they have in-house quality control mechanisms to protect the data.

Organisation Y uses insurance data from insurance companies, rather than from insured persons. Health insurance companies are the clients of Organisation Y. Organisation Y identifies itself as responsible for the data and conducts quality analysis of it as much as necessary to comply with the informed consent of the insurer and with the goals identified between Organisation Y and the insurance company. Organisation's Y responsibility is directed to the insurance company but not the insured person.

5.4. Ownership of Data

Organisation X has no issue with ownership of the data, because they clearly understand and identify that the data used for identification of fraudulent claims and for claims analysis is the data from insured persons and it is their (the insured person's) data. Although in practice there are situations (for example, when using the data for fraud detection) when they say that:

“The respective person perhaps does not know that they use the data for fraud detection” (Interviewee X, 2018)

Organisation X works according to all national and European data protection regulation laws, so they don't identify any problems in these situations, but a possible ethical concern may be, that the insured person isn't informed, what is being done with his/her personal information.

For Organisation Y, which uses insured persons' data for analysis to make information products (predictive models, recommendations how to improve administrative processes in healthcare, etc.) for health insurers, the situation is perceived to be completely different. Organisation Y uses data of insured persons' (e.g. personal data and insurance data) but they identify it as the property of the insurance company, not of the person. Interviewee from Organisation Y said that insurance companies are responsible for ensuring that insured people are informed as to how their data is used. Organisation Y gets informed consent from insurance companies as their clients. They conclude an agreement, which states the goals of the relationship and elaborates the uses of the insurance data. Organisation Y does not worry whether insured persons know of the relationship. Organisation Y states that their work is transparent, that they are working according to the data protection regulation and also they have annual audits to ensure that their software is working properly. They give information about the use of insurance data in their website for the public, but they identify the insurance data as the property of the insurance company. As the interviewee stated, *“it's their data”*.

5.5. Transparency

Organisation X states that smart technology used in the organisation is more or less transparent for both the direct users and the personnel working with smart information systems (IT department). However, the smart technology used in the organization is not transparent to people outside the organization because Organisation X does not inform those people as to how smart information system in their organization works. For example, a person outside the organisation doesn't get the information about the criteria of how one or another claim is identified as fraudulent. Also clients are not always aware why smart technology makes one or another decision, but they are informed on the general level as to how it works.

Organisation Y tries to be as transparent as possible for the stakeholders: the insured persons, health insurance companies, and universities. Moreover, they have rules in the software itself. Yearly audits made by an external auditor also help to ensure transparency in Organisation Y.

In both organisations (Organisation X and Organisation Y) all stakeholders have the ability to share any concerns with the organisation – if they find some aspects concerning transparency in data collection, data analysis, informing about handling personal

information troubling, they always have a possibility to share them. In Organisation's X situation there is a board of directors which can give their feedback about the processes in the company (including the software), and a quality control mechanism to ensure that everything is working as it should. Organisation Y gets feedback from insurance companies. As they say

"We are trying to be as transparent as possible" (Interviewee Y, 2018)

"If they have problems they will directly tell us" (Interviewee Y, 2018)

5.6. Trust

Trust is very important for Organisation Y. Health insurance companies are their main clients and it is very important for Organisation Y that health insurance companies would trust them. They are less concerned about the trust of insured persons, but that follows from the specifics of their functions.

It is very important for Organisation Y to follow the goals agreed between them and the health insurer,

"We follow their orders" (Interviewee Y, 2018)

They also send requests to health insurance companies every month to get their consent for using insurance data for other purposes, for example meeting requests from universities or institutes to use the data for research. Organisation Y states that they do not do anything without the consent of the health insurer.

5.7. Informed Consent

Organisation X uses personal information of insured persons in the identification of fraudulent claims. Interviewee X said that there is no specific informed consent is sought for using their personal information for this purpose. Although Organisation X does not see a problem, that the person isn't informed clearly about this use of his/her personal information in that as they are working according to the data protection regulation of Germany and of the European Union.

Organisation Y has legal restrictions on its use of personal and insurance data of insured persons. As the interviewee stated,

"Every time they are using the data for something they have to ask for the health insurers if they agree" (Interviewee Y, 2018)

Organisation Y does not have an obligation to get informed consent from insured people whose data they use. On their behalf, health insurance companies have to get informed consent from insured people. Organisation Y gets the data directly from the

insurance companies: as they say, *“it’s their data”*. The only informed consent Organisation Y is concerned, is the informed consent of the insurance company.

5.8. Use of Personal Data and Security

Both Organisation X and Organisation Y use personal data of insured persons to achieve their goals. Organisation X uses it for fraud detection and claims analysis, Organisation Y for making information products for insurance companies and research data for universities and institutes.

To address possible ethical issues associated with the use of personal data of insured persons, Organisation X is working according to the data protection regulations of Germany and the European Union. Although there is no organisational policy for use of personal data in the Organisation X. Additional in-house mechanisms to ensure maximum security of the data used by the software for fraud detection are employed. They have a set of rules to use the software properly and a quality control system, which they apply to every process of their work.

Organisation Y, besides legal instruments (national, European and organisational), has an external auditor which conducts audits of the system and other processes every year, to ensure that everything is working properly. They also have implemented rules directly in the software to ensure security. They also send requests to health insurance companies every month to get their consent for using insurance data for other purposes, for example meeting requests from universities or institutes to use the data for research. Organisation Y states that they do not do anything without the consent of the health insurer. Organisation Y has also implemented rules directly in the software to ensure proper use of personal data.

All in all, both Organisation X and Organisation Y have mechanisms to address possible use of personal data and security issue, but they only tackle those aspects, which they identify as more important for the organisation. For example, Organisation X doesn’t have any organisation policy for the use of personal information. Also, they state, that Organisation X is working according to the European Data Protection Regulation, but Organisation X doesn’t have an internal mechanism to ensure that. In the Organisation Y, the main concern is not the person himself/herself whose information is being used for the analysis, but only the information of the insurance company which is the direct client of the Organisation Y. All these remaining issues should be addressed in the future.

6. Conclusion

From 2016, more has been invested into implementing mart information systems in the insurance sector than any other. Today half of the insurance companies in the world are looking at strategic alliances or joint ventures with InsurTech companies to speed up their alignment with the digital marketplace. This case study demonstrates where smart information systems are being used in the insurance sector, why they are required, what

benefits and what possible harms they could bring to companies, employees and the customers. Despite the need of implementation of smart information systems which is understood as needed to compete with other insurance companies, there are many social and ethical issues that need to be addressed in the implementation of smart technologies in the sector.

The interviews show that when using smart technologies in the insurance sector some ethical issues identified in the literature are not emphasized as significant or not identified as issues at all in the interviews (such as bias, reliability, discrimination, data governance, security and privacy, job losses). However, some ethical issues were not mentioned as significant in the literature but were identified as very important during the interviews (e.g. trust, informed consent, responsibility). Transparency and accessibility of data as ethical issues appeared to be important in both literature and practice.

Of course, there is a possibility that such conclusions are associated with the different backgrounds of the interviewees, but their roles in the organisations are significant and broad, so their knowledge on the ethical issues should be considered as similarly significant. Also the mentioned issues could seem less important to the interviewees, because there is no clear legislation on those. Both organisations (Organisation X and Organisation Y) are private ones, so possibly their view on ethical issues is more practical - possibly they acknowledging only those issues, which can bring legal amenability and disrupt their work. If not – they are considered as not so important.

It is worth mentioning that both interviewed companies (Organisation X and Organisation Y) are putting considerable energy into addressing the issues identified by, for example, conducting annual audits, collecting feedback from staff and clients, cooperating with the board of directors, and following European, national and company regulations. Those smart information systems related internal issues, that have not yet been identified by organisations in the insurance sector, should be identified and addressed in the near future. That is a crucial part for ensuring flawless implementation of smart technologies and further use in the insurance sector, without harming neither the insured persons, nor other insurance companies and employees. Moreover the literature review and the case study has shown, there are few if any policy documents for using SIS in the insurance sector. The only policies used are General Data Protection Regulation and other national policies on data protection. But data protection and privacy are important topics in the context of smart information systems in insurance. Therefore, it is important to create at least national policies on using smart technologies in insurance and implement the findings from this case study.

6.1. Limitations

There are no limitations of the technology itself, according to the organisations (Organisation X and Organisation Y) the software works fluently. Two significant limitations were raised in working with the software. First is the possibility of identifying strange or unusual behaviours of insured persons as fraudulent even if they are not (false positives). This is the limitation which is acknowledged by Organisation X, and explains why any final decision is still made by a human. The software merely identifies claims with a high possibility of fraud. After that a human goes through the claim and confirms that the software made the right decision. Organisation X has quality control systems to minimize the possibility of this kind of mistake, but the limitation still exists and must be acknowledged by the organisation and its employees. That the final decision is still made by humans resolves this limitation for the time being.

Another identified limitation is data collection. Organisation Y highlighted that the software is not able to get information for the analysis itself. It must be manually collected from insurance companies. The software only analyses collected information. It is important to state that there is a strong link between accuracy of data and accuracy of recommendations. Organisation Y provides insurance companies or other interested institutions (universities, institutes) with information products which they can use in research or developing policies in health insurance. Although, Organisation Y does not see it as an very important limitation for the company, because it makes information products only for those insurance companies who provided the information so actively nothing is being done to address this limitation. In the future, though, there should be some measures to control the quality of the information because the results of the analysis are sometimes used by other institutions (universities, other research institutions) in research.

6.2. Contribution to Knowledge

The findings of this case study could make a significant contribution to existing knowledge on ethical issues when using smart information systems in the insurance sector. One reason has been stated in the literature review - CEOs of insurance companies see great benefits of SIS (e.g. personalised interactions with customers, higher customer satisfaction, and financial savings). That means that in the near future smart technologies in the insurance sector are going to be a necessity if a company wants to compete in the field and the implementation of them will rise very fast.

Another reason has been found in the interviews. They have shown that when using smart information systems in the insurance sector some ethical issues identified in the literature are not emphasized as significant or not identified as issues at all in the interviews (such as bias, reliability, discrimination, data governance, security and privacy, job losses). However, some ethical issues were not mentioned as significant in the literature but were

identified as very important during the interviews (e.g. trust, informed consent, responsibility). Transparency and accessibility of data as ethical issues appeared to be important in both literature and practice. That shows that the theoretical knowledge of implementing smart information systems into the insurance sector and possible issues rising in the process differs from practice. Findings of this report could help to broaden the theoretical perspective of this situation and highlight other possible issues (e. g. lack of smart technologies related ethical knowledge in organisations, technologically oriented approach into the situation).

6.3. Implications of This Report

This report uses information from insurance companies using SIS in practice so the findings are highly significant. The differences between the consideration of importance of the ethical issues identified in the literature and in the interviews hopefully will provide guidance to the insurance companies integrating smart information systems. Moreover, the findings of this report will encourage insurance companies to analyse the situation in their organisations more closely before implementing smart information systems in their practice and help them to understand that smart technologies are not only tools to make their life better, but also tools of great responsibility, which, if not used properly could harm not only the company but also the insured people. Hopefully, in the future, the results of this report also provide policymakers with information about possible issues when using SIS in the insurance sector.

6.4. Further Research

This report offers a literature review and findings on the case study on ethical and legal issues when using smart information systems in the insurance sector from both theoretical and practical perspectives, although there may be additional matters that need to be evaluated in the future. Additional case studies would be needed to evaluate the differences of ethical and legal issues between other types of companies (for-profit and not for-profit, huge corporations and small organisations, etc.).

It is substantial for companies in the insurance industry to acknowledge all ethical problems identified in this report as significant ones. There are already many recommendations developed to address ethical issues when using smart technologies in insurance, but the problem is that it is not known how to implement those recommendations into policy. Much more research should be done on the best possible ways to implement theoretical recommendations into policy and then into practice (e. g. practical examples, case studies, simulations, theoretical approach).

The conclusions of this report should encourage conducting similar case studies and provoke qualitative and quantitative studies in broader range of insurance companies, countries, smart technologies to get as most reliable results as possible in the future.

7. References

1. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H. and Saadi, M. (2018). *Big data security and privacy in healthcare: A Review*. [online] www.elsevier.com. Available at: <https://reader.elsevier.com/reader/sd/pii/S1877050917317015?token=D846E08C5FCA82A132324DA47B16E00EF7AC2C5A61B478FBE93AEF1CF8078D12C23F10C9A396316D202DF07A27B3FE32> [Accessed 9 Nov. 2018].
2. Accenture (2018). *Future Workforce Survey – Insurance. Realizing the Full Value of AI*. [ebook] Accenture. Available at: https://www.accenture.com/t00010101T000000Z__w__/gb-en/_acnmedia/Accenture/Conversion-Assets/NonSecureClients/Documents/PDF/3/Accenture-Future-Workforce-Survey-Insurance-Report.pdf [Accessed 9 Nov. 2018].
3. Bharadwaj, R. (2018). *How Insurance Leaders Can Prepare for Artificial Intelligence Today* -. [online] TechEmergence. Available at: <https://www.techemergence.com/insurance-leaders-can-prepare-artificial-intelligence-today/> [Accessed 9 Nov. 2018].
4. Clover Health (2018). *Clover Health | About Clover*. [online] Cloverhealth.com. Available at: <https://www.cloverhealth.com/en/why-clover/about-clover> [Accessed 9 Nov. 2018].
5. Deloitte Digital (2017). *From mystery to mastery: Unlocking the business value of Artificial Intelligence in the insurance industry*. [online] Www2.deloitte.com. Available at: <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-artificial-intelligence-in-insurance-whitepaper.pdf> [Accessed 9 Nov. 2018].
6. Dutt, R. (2018). *Why artificial intelligence in health care is harder than you would think*. [online] InfoWorld. Available at: <https://www.infoworld.com/article/3269197/artificial-intelligence/why-artificial-intelligence-in-health-care-is-harder-than-you-would-think.html> [Accessed 9 Nov. 2018].
7. Expert System (2018). *The advantages of using AI in Insurance | Expert System*. [online] Expertsystem.com. Available at: <https://www.expertsystem.com/advantages-using-ai-insurance/> [Accessed 9 Nov. 2018].
8. Foggan, L. and Panagakos, E. (2018). *AI in insurance: New opportunities come with new worries | PropertyCasualty360*. [online] PropertyCasualty360. Available at: <https://www.propertycasualty360.com/2018/05/08/ai-in-insurance-new-opportunities-come-with-new-wo/?slreturn=20181009024138> [Accessed 9 Nov. 2018].

9. Koh, H. and Tan, G. (2018). *Data Mining Applications in Healthcare*. [online] Citeseerx.ist.psu.edu. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.92.3184&rep=rep1&type=pdf> [Accessed 9 Nov. 2018].
10. Lemonade Insurance Company (2018). *How Lemonade's Tech-Powered Claims Work / Lemonade*. [online] Lemonade.com. Available at: <https://www.lemonade.com/claims> [Accessed 9 Nov. 2018].
11. Lerner, M. (2018). *Insurers urged to integrate artificial intelligence with human workforce - Business Insurance*. [online] Business Insurance. Available at: <https://www.businessinsurance.com/article/20180510/NEWS06/912321204/Insurers-urged-to-integrate-artificial-intelligence-with-human-workforce> [Accessed 9 Nov. 2018].
12. Marr, B. (2018). *How Big Data Is Changing Insurance Forever*. [online] Forbes. Available at: <https://www.forbes.com/sites/bernardmarr/2015/12/16/how-big-data-is-changing-the-insurance-industry-forever/#4169df22289b> [Accessed 9 Nov. 2018].
13. Newton Media (2018). *Revolutionising claims handling and fraud detection with AI*. [online] Intelligent Insurer. Available at: <https://www.intelligentinsurer.com/news/revolutionising-claims-handling-and-fraud-detection-with-ai-13318> [Accessed 9 Nov. 2018].
14. Progressive Casualty Insurance Company (2018). *Progressive: Ranked One Of The Best Insurance Companies*. [online] Progressive.com. Available at: <https://www.progressive.com/home/adaptive/> [Accessed 9 Nov. 2018].
15. Sennaar, K. (2018). *How America's Top 4 Insurance Companies are Using Machine Learning -*. [online] TechEmergence. Available at: <https://www.techemergence.com/machine-learning-at-insurance-companies/> [Accessed 9 Nov. 2018].
16. Shift Technology (2018). *Solutions - Shift Technology*. [online] Shift Technology. Available at: <https://www.shift-technology.com/solutions/#force> [Accessed 9 Nov. 2018].
17. Shift Technology (2018). *Solutions - Shift Technology*. [online] Shift Technology. Available at: <https://www.shift-technology.com/solutions/#luke> [Accessed 9 Nov. 2018].
18. Tata Consultancy Services (2017). *TCS Global Trend Study on Artificial Intelligence Reveals Industry Wide Investment by 2020*. [online] Available at: <https://www.tcs.com/global-trend-study-artificial-intelligence-reveals-industry-wide-investment-2020> [Accessed 9 Nov. 2018].
19. Tata Consultancy Services Ltd (TCS) (2017). *Getting Smarter by the Sector: How 13 Global Industries Use Artificial Intelligence*. Tata Consultancy Services Ltd (TCS).

20. Trov, Inc. (2018). *About Us*. [online] Trov.com. Available at: <https://www.trov.com/about> [Accessed 9 Nov. 2018].
21. Wiens, C. (2018). *Getsafe launches its Digital Health Insurance – Getsafe*. [online] Getsafe. Available at: <https://blog.getsafe.eu/nr-2-3-getsafe-launches-its-digital-health-insurance-9d90a11242df> [Accessed 9 Nov. 2018].
22. Zagorin, E. (2018). *Artificial Intelligence in Insurance - Three Trends That Matter -*. [online] TechEmergence. Available at: <https://www.techemergence.com/artificial-intelligence-in-insurance-trends/> [Accessed 9 Nov. 2018].

CS07 – Energy and Utilities



Case Study: Smart Grids and Ethics



This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641



Document Control

Deliverable	Deliverable 1.1.: Case Studies
WP/Task Related	WP 1: Representation and Visualisation
Delivery Date	31 January 2019
Dissemination Level	Public
Lead Partner	Trilateral Research
Contributors	Tally Hatzakis; Rowena
Reviewers	Mark Ryan, UT
Abstract	This report provides an overview of the current implementation of SIS in the field of smart grids. It also identifies the positive and negative aspects of using SIS in smart grids, including ethical issues which could arise while using SIS in this area. One company working in the industry of telecommunications (Liander) is analysed in this report. Further specific ethical issues that arise when using SIS technologies in Liander are critically evaluated. Finally, conclusions are drawn on the case study and areas for improvement are suggested.

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes
0.1	14/11/Y2018	Tally Hatzakis	Rowena Rodrigues	First Draft / Review etc. Circulation: Consortium/ Marlou Kevin McNiche Mark Ryan
0.2	22/12/2018	Tally Hatzakis	Marlou Kevin McNiche Mark Ryan	Second Draft/Review Circulation: Consortium Partners
0.3	18/01/2019	Tally Hatzakis	Doris Schroeder	Third Draft/Review Circulation: Consortium

Contents

Executive Summary	199
Smart Grids and Ethics: A Case Study	200
1. The Use of SIS in Smart Grids	201
2. Ethical issues of using SIS in smart grids	207
2.1 Health and Safety: Does the smart grid make us unhealthy?.....	208
2.2. Privacy and Informed Consent: Does the smart grid give away household privacy?	208
2.3. Cyber-risks and Security: Do we jeopardise energy security?	209
2.4. Affordability and energy equity: A new criteria to set society apart.....	210
2.5. Sustainability: Doing our bit for climate change	210
3. Liander: The Case of a Large Distribution System Operator using SIS in Smart Grids	211
3.1. Description of Liander	211
3.2. Description of SIS technologies used in Liander	213
3.3 The effectiveness of using SIS for Liander	215
4. Liander: Ethical issues from SIS Technology	216
4.1 Privacy and informed consent	216
4.2 Security of the smart grid.....	217
4.3 Other issues.....	218
4.4 Mechanisms for addressing ethical issues.....	219
5. Conclusion	219
5.1. Implications of this Report.....	220
5.2 Further Research.....	220
6. References	220

Executive Summary

This case study explores the principal ethical issues that occur in the use of Smart Information Systems (SIS) in smart grids and offers suggestions as to how they might be addressed. Key issues highlighted in literature review have been reviewed and the views of two interviewees employed in Liander have been accounted for. The aim of this case study is to identify which ethical issues arise from the use of SIS in cybersecurity, the current efforts for the organisation to address them, and whether practitioners are facing additional issues not addressed in current literature. The literature review highlighted mainly ethical issues around health and safety, privacy and informed consent, cyber-risks and energy security, affordability and equity, sustainability. The key topics raised by interviewees evolved around privacy and to some extent cybersecurity. This may be due to the prevalence of the issue within the sector and the company in particular or due to the positions held by interviewees in the organisation. Issues of sectorial dynamics and public trust, codes of conduct and regulation which are not discussed in the literature. The case study hence highlights the ability of case studies to identify ethical issues not covered (or covered to an inadequate degree) in academic literature and yet which are facing practitioners in the energy sector.

Smart Grids and Ethics: A Case Study

“As a crucial element of our overall energy and climate strategy, we need to ensure that our energy infrastructure is sustainable, goal-oriented and operational.”

Miguel Arias Cañete, Commissioner for Climate Action and Energy

The energy sector represents the critical infrastructure upon which all other economic activities, modern life conveniences and services, including the wide spectrum of information and communication technologies (ICT) are based. The expected demands on the energy sector over the coming years will be immense, due to the proliferation of ICT technologies and their ubiquitous use in all aspects of social and economic life.

Many factors will increase society’s electricity demands in Europe, such as the advent of Internet of Things⁴⁴ (IoT) sensors, the increased digitalisation of social life due to robotics and blockchain⁴⁵, the further digitalisation of industry, and the transition from fossil fuel-powered to electric cars. In parallel, to tackle climate change and decrease reliance on imported fossil fuels, Europe is pushing for greater integration of renewables in the mix of energy production sources. In combination, both put great pressure on the capacity of Europe’s pre-existing energy distribution network infrastructure, which cannot currently scale up to meet expected demands, at least not if managed in traditional ways. European countries have two options (EC Com 356, 2014):

- a) invest in upgrading energy infrastructure networks; or
- b) optimise the use of the existing infrastructure capacity by utilising SIS.

On the supply side, improved efficiency can derive from better management of volatile renewable energy generation solutions, improved maintenance of the energy grid infrastructure, and even enhancing modelling of demand needs and thereby infrastructure investments. On the demand side, improved efficiency can derive from shifting energy consumption patterns through real-time demand-response pricing and load balancing across the grid (EC, 2016).

While the use of SIS systems in energy distribution, i.e. in smart grids, hold the promise that countries will be able to ensure affordable and sustainable energy for the ever-increasing energy demands of smart living (EC, 2016), it presents a number of ethical challenges (Sarvapali, et.al, 2012).

This case study reviews the social, ethical, and human rights issues arising from the utilisation of SIS systems (AI technologies and big data analytics) in the energy sector and in particular in smart energy grids. Section 1 explains the use of SIS in the energy sector and in particular in energy distribution via energy grids. Section 2 will review the current implementation of big data and AI-powered analytics in the energy sector and the ethical issues that may arise as a result. It will focus on the types of SIS technologies being used and highlight the range of social and ethical issues surrounding their use.

⁴⁴ “The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data”. Source: https://en.oxforddictionaries.com/definition/internet_of_things

⁴⁵ “A system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network.” Source: <https://en.oxforddictionaries.com/definition/blockchain> The term is now used for recording exchanges beyond cryptocurrency.

Section 3 will analyse Liander, a Dutch utility company. Section 4 will explore and critically evaluate ethical issues arising from the introduction of SIS technologies in smart grids in practice, through interviews conducted with Liander staff members. This section will evaluate whether there are policies and procedures in place to tackle these issues, and what the protocol is for addressing concerns.

1. The Use of SIS in Smart Grids

The use of SIS systems in energy promises to ensure sustainable affordable energy for the ever-increasing demands of smart living without big investments in the energy distribution systems in two ways. First, SIS systems allow to optimise the management of energy demand and energy supply from existing resources. Smart grids involve a host of intelligent technologies to improve the management of the energy distribution network that connects energy producers with consumers. These include:

- sensors that collect real-time information about energy quality at different points along the distribution network,
- sensors that collect information about consumption via smart meters installed in people's houses,
- mechanism to analyse all collected data in order to better predict energy needs, optimise supply and demand and swiftly respond to unpredicted changes in either, and
- finally means to provide the necessary insights to design incentivisation programmes to change energy consumption behaviours.

Second, smart grids enable the safe incorporation of renewables and green electricity into the grid. While renewables are a key component of Europe's sustainability goals, their integration poses a challenge for traditional power grids. Surges of power generated by renewables may overcharge the grid leading to power cuts and costly maintenance work, or compromise the reliability and quality of the electricity provided (Rathi, 2017). SIS systems allow to safely manage the risks from integrating renewables into the energy production mix. According to Liang (2017), quality issues arise from:

- voltage and frequency fluctuations that can be caused by the intermittent nature of renewable energy production due to changing weather conditions and
- harmonic (wavelength) distortions introduced by electronic devices utilised in renewable energy generation.

Such risks introduced by renewable energy technologies may affect the performance of electrical equipment, particularly sensitive electronic devices. A number of problems can compromise the performance and reliability of electronic systems, such as equipment shutoff, errors or memory loss, loss of data and burned circuit boards, reader errors and the like. To handle such volatility requires the monitoring and control of electricity from the point of production to the point of consumption, as well as real-time adjustments in energy distribution depending on fluctuations in weather conditions, fluctuations in energy generation and demand and other factors that can affect the quality of the energy supply (Rojin, 2013). Hence, the use of smart grid technologies can help solve the Energy Trilemma: how to secure (energy security) affordable energy for all (energy equity) in a sustainable manner (environmental sustainability).

Energy security: Effective Management of primary energy supply from domestic and external sources, reliability of energy infrastructure, and ability of energy provide to meet current and future demand.

Energy equity: Accessibility and affordability of energy supply across the population.

Environmental Sustainability: Encompasses achievement of supply- and demand-side energy efficiencies and development of energy supply from renewable and other low-carbon sources.

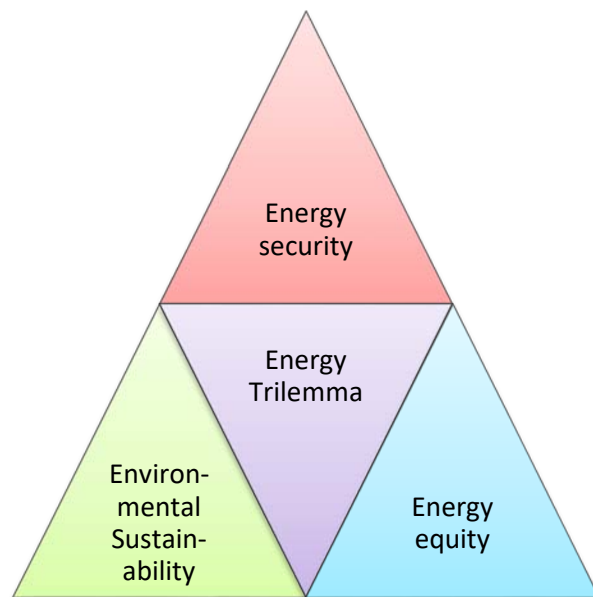


Figure 1: The three dimensions of the energy trilemma. Source: World Energy Trilemma Index 2018, World Energy Council 2018 at: <https://trilemma.worldenergy.org/reports/main/2018/2018%20Energy%20Trilemma%20Index.pdf>

The application of SIS in the energy sector in Europe is deployed within the wider context of accelerating the European Energy System transformation set out by the Integrated Strategic Energy Technology Plan (SET-Plan) (EC, 2016). The SET plan was originally conceived in 2008, and amended in 2015 to introduce steps towards a pan-European Energy Union. It seeks to accelerate knowledge and technology transfer and adoption, foster research and development (R&D), and drive the uptake of low-carbon energy technologies to reach energy and climate change goals and achieve the transition to a low carbon economy by 2050 (EC, 2016). The plan makes provisions for dealing with the technological challenges posed by renewables, their volatility in energy production and their distributed nature. It also makes provisions for the integration of the upcoming electric transport systems and IoTs in an integrated energy system, which will require new protocols of data exchange and collaboration across the energy, transport, and ICT sectors and regulators. The plan sets out a number of priorities to facilitate innovation in the sector with the view to develop and implement solutions that can help (a) maximise the value and lifetime of the existing grid to defer large lump sum investments in costly new infrastructure, and (b) integrate power from renewable generation sources and distribute it at a local or regional level (see Figure 2 below).







Energy Union <i>Research, Innovation and Competitiveness Priorities</i>		SET-Plan 10 Key Actions
No1 in Renewables		1 Performant renewable technologies integrated in the system 2 Reduce costs of technologies
Consumers in the Energy System		3 New technologies & services for consumers 4 Resilience & security of energy system
Efficient Energy Systems		5 New materials & technologies for buildings 6 Energy efficiency for industry
Sustainable Transport		7 Competitive in global battery sector and e-mobility 8 Renewable fuels and bioenergy
Carbon Capture Utilisation and Storage		9 Carbon Capture Storage / Use
Nuclear Safety		10 Nuclear safety

FIGURE 2: TOP 10 PRIORITIES OF THE SET PLAN RATIFIED IN TALLINN 2016. SOURCE: EC (2016) TRANSFORMING THE EUROPEAN ENERGY SYSTEM THROUGH INNOVATION: INTEGRATED STRATEGIC ENERGY TECHNOLOGY (SET) PLAN PROGRESS IN 2016 (DOI:10.2833/661954), LUXEMBOURG: PUBLICATIONS OFFICE OF THE EUROPEAN UNION, 2016

Smart grids involve a host of intelligent technologies to improve monitoring and control of energy consumption, and communication technologies to address operational issues around distribution and production, but also collect real-time information about energy consumption from consumers via smart meters. It is worth noting that such technologies do not substitute but complement traditional grids. Such technologies comprise:

- HAN (Home Area Networks), which ensure the communication between smart meters and smart appliances
- WASA (Wide Area Situational Awareness) which provides monitoring of performance and ensures dynamic prevention and response services when necessary.
- SCADA (Substation Supervisory Control and Data Acquisition) systems, which are used to monitor and control energy plants or equipment, as well as transportation.

- AMI (Advanced Metering Infrastructure) which allows smart meters to communicate with the grid.
- PMUs (Phasor Measurement Units) which allow the concurrent, real-time monitoring of energy supply systems by measuring electricity current and voltage by amplitude and phase across selected locations (stations) of the grid.
- WAMPAC (Wide Area Monitoring Protection and Control) which ensures the security of the power system.
- IEDs (Intelligent Electronic Devices), smart devices which can communicate with each other and with SCADA to enable fault detection and rectification.
- FACTS (Flexible AC Transmission Systems, such as Unified Power Flow Controllers), which enable long distance transport and integration of renewable energy sources.

Energy data from a variety of sources is combined and analysed (ENSI 2016), in order to:

- **Develop a responsive power grid** to achieve appropriate levels of reliability, resilience and economic efficiency in the face of the fluctuations of renewable power generation. Smart power grids optimise not only the seamless integration of sustainable power, but also its storage, its connection with other networks (e.g. heat and cold, transport), and the inter-regional exchange of power.
- **Develop local and regional energy systems** to facilitate the integration of renewables in the local or regional supply by 2030, and enable the inter-regional exchange of spare energy, as well as the security and resilience of European energy systems (see Figure 3 below) .

Smart grid management systems require the analysis of real-time energy consumption data and energy production data. AMI collect household energy consumption data, as well as data relating to voltage quality, power quality, active energy and reactive power, as well as diagnostics information about the condition and control of the smart meter itself (pinging the meter) and operational status (indicators, alarms and error messages) from the meter.

The use of artificial intelligence and big data analytics in the energy sector is nascent. It is contingent upon the widespread adoption of smart meters by the public. According to an EC study (2014), there were 45 million electricity smart meters installed in Finland, Italy and Sweden representing only 25% of the potential market penetration in these countries. This number has increased to around 60% by 2018, but still falls behind the expected levels of smart meter penetration of 80% that is necessary to require and justify the use of such systems for energy management. Nevertheless, progress towards this goal is likely to be rapid. In 16 European Member States (Austria, Denmark, Estonia, Finland, France, Greece, Ireland, Italy, Luxembourg, Malta, Netherlands, Poland, Romania, Spain, Sweden and the UK) rollouts of smart meters by 2020 or earlier are planned, and Poland and Romania have already seen consumer benefits.

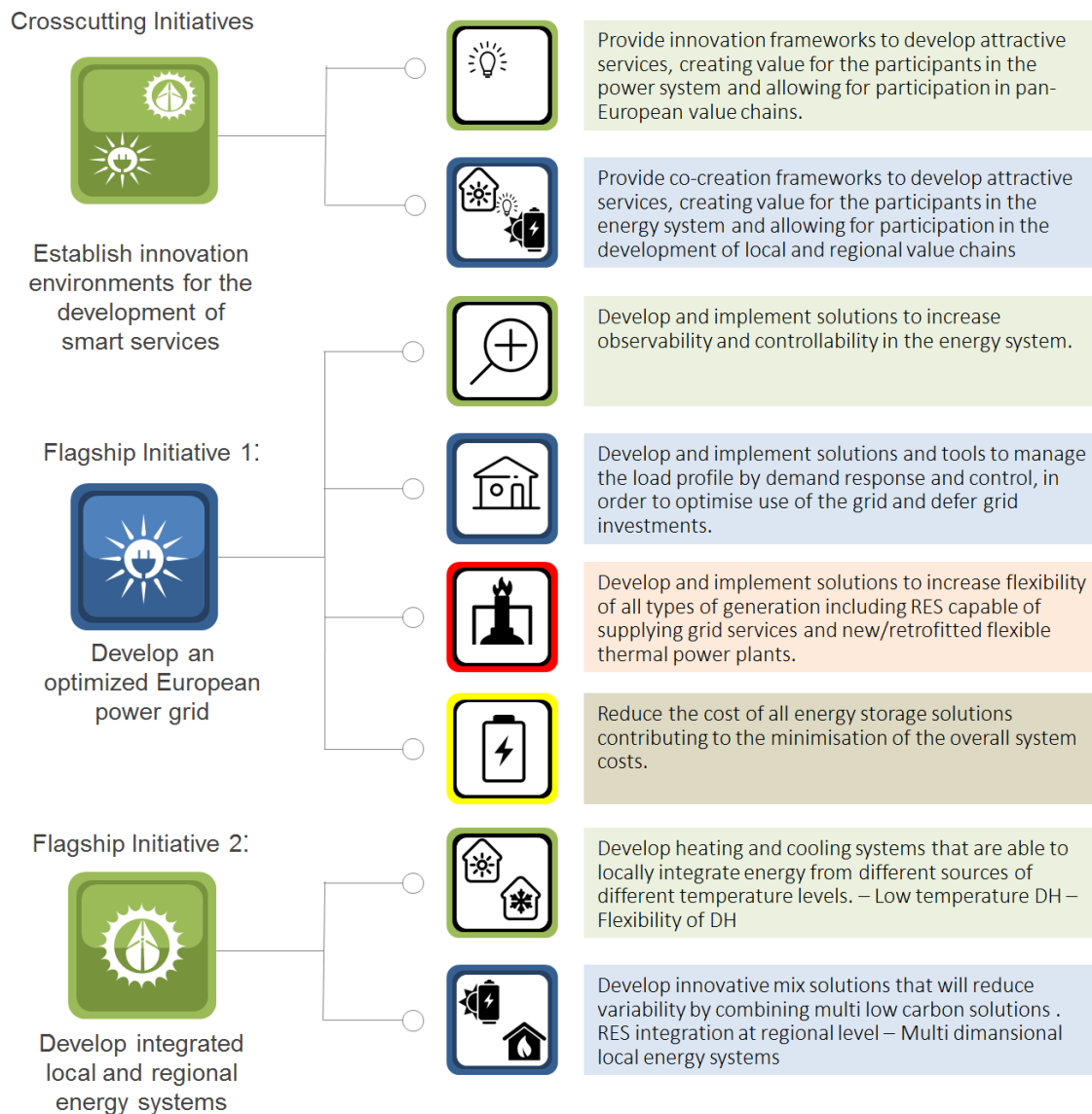


Figure 3: Current Innovation Priorities of SET plan Source: Regulatory Innovation Zones for Smart Energy Networks
Source: ENSI (2018) Regulatory Innovation Zones for Smart Energy Networks [online] Available at <https://www.youtube.com/watch?v=JyR9aitMfIU> [Accessed 27 Nov, 2018]

In Germany, Latvia and Slovakia, smart metering was found to be economically justified, but only for particular groups of customers, while the business case in terms of consumer benefits across the population was either negative or inconclusive in Belgium, the Czech Republic, Germany, Latvia, Lithuania, Portugal, and Slovakia. No roll out plans were available in Bulgaria, Cyprus, Hungary and Slovenia. In 15 of the 16 Member States, distribution system operators (DSOs) are responsible for installing smart meters in households which are to be financed via network tariffs⁴⁶. DSOs are responsible for energy distribution infrastructure (mainly electricity and gas pipes, exchanges, etc.). Not only are DSOs responsible for installing the meters, but also for data analytics in most countries, with the exception of Denmark, Estonia, Poland and the UK, where data will be handled by an

independent central data hub; and with the exception of Czech Republic, Germany and Slovakia where alternative options for data handling are being considered. The European Commission requires that companies advise customers on how best to balance their energy consumption and enable new energy related services and products. This hinges on access to real-time customer information and raises issues of profiling due to the gathering and storing of sensitive information on the household energy footprint, and stored data in the light of privacy and confidentiality policies (EC Com 356, 2014).

The European Energy Union aspires to connect different country networks in an integrated energy system. This will require data and knowledge exchange as well as collaborations across the energy, transport, and ICT sectors, experts and regulators transnationally. The stakeholder landscape in the energy sector is beginning to change, giving rise to the development of cross-sectoral and cross-country collaborations, such as the European Technology and Innovation Platform on Smart Networks for the Transition, with the participation of industry representatives, research, academia, and users (see Figure 4 below). The development of cross-border groups is an interesting development in that there is an international collaboration between DSOs to tackle common issues, which is of particular interest to the case below. Platforms for a public debate with the participation of all types of future energy providers might be more useful in voicing concerns, getting public commitments towards agreed courses of action and informing policy and regulations.

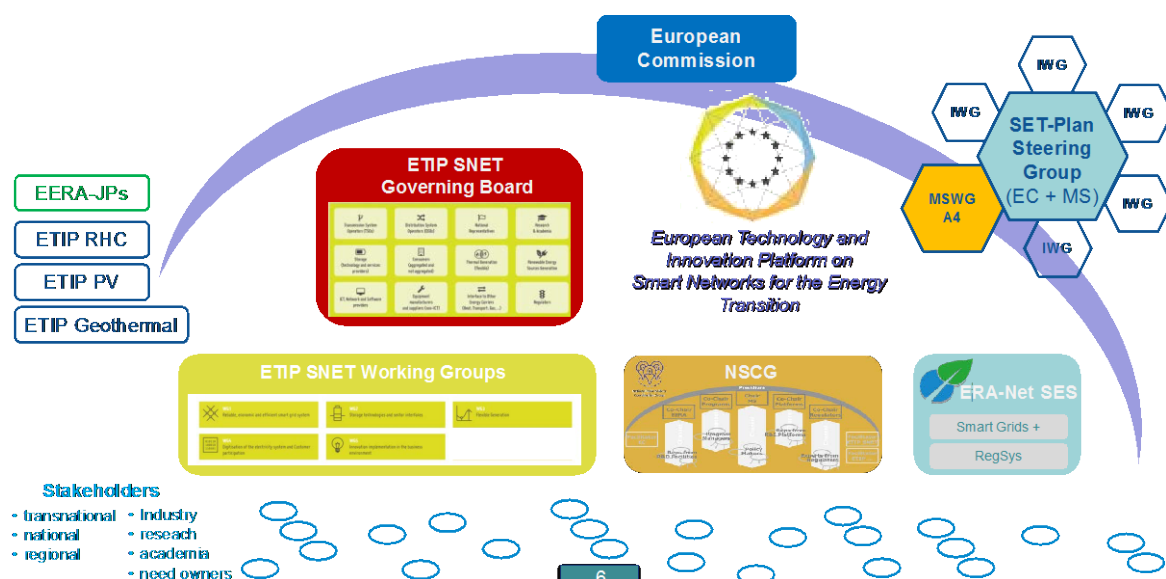


FIGURE 4: THE SMART GRID INNOVATION LANDSCAPE: THE EUROPEAN TECHNOLOGY AND INNOVATION PLATFORM ON SMART NETWORKS FOR THE TRANSITION INVOLVES INDUSTRY REPRESENTATIVES, RESEARCH, ACADEMIA, AND USERS. SOURCE: [HTTPS://SETIS.EC.EUROPA.EU/SYSTEM/FILES/COMMUNICATION_SET-PLAN_15_SEPT_2015.PDF](https://setis.ec.europa.eu/system/files/communication_set-plan_15_sept_2015.pdf)

Not only does the relationship between companies within the energy supply chain is beginning to change, but also the relationship between companies and customers. Smart utilities promise consumers greater control over their energy consumption choices by collecting and providing customers with real-time information related to energy use and pricing. In addition, the role of end users in the energy value chain is likely to change. With the advent of household renewables solutions,

end users will increasingly generate their own power to use, give back to the grid or exchange at a local level. Hence their role will increasingly change from that of passive consumers of energy to that of an energy prosumer⁴⁷. This will require the development of smart household energy management and billing systems that can become an extension of the existing energy grid (IEA, 2017).

Typically, end users receive their household energy from energy providers (gas and electricity companies) with whom they have a contract agreement. Many such utilities struggle to garner their customers' support for the installation of smart meters in households, particularly in Europe and the USA. The two primary concerns fuelling the resistance to smart meters relate to health and data privacy issues. Customers, in general, are uncomfortable with commercial organisations, including utilities, possessing such fine-level data that can give away intimate information about one's lifestyle (EC Com 356, 2014). Aside from privacy, a number of other ethical issues relate to the use of SIS in smart grids.

2. Ethical issues of using SIS in smart grids

Despite the wide range of articles on smart grids, there has been very little research on the ethical and legal implications of using SIS technologies in energy. The installation of smart meters in the mainstream is not completed. Consumer research that has taken place relies mostly on pilots with interested parties and looks at the response and use of such technologies, from a functional rather than an ethical perspective. There have been few articles that have cohesively addressed ethical issues of SIS technology in the energy sector. A key issue receiving little attention at present is the implications of energy grids for energy justice and transitional justice to smart grids. Smart grids and their management are only a part of the new energy ecosystem and will likely become the key customer platform and key industry gatekeeper collecting customer insight. There seems to be an underlying mistrust towards energy players and governments about their positions and commitments towards practices that benefit society as a whole once implementation takes place.

Anticipated consumer benefits, such as energy savings, are predicated on the collection and analysis of granular information on household energy usage via smart meters, but these can be used to reveal detailed information about people's private lives within the home, raising serious questions at a technical and policy level about in-home surveillance and how to address consumers' privacy interests. These issues have been particularly controversial for gaining user acceptance in the US and Europe (Weaver, 2014). In addition, energy systems are strategic targets for economically-motivated cybercrime, cyberterrorism, and even cyberwar. Smart grids have ICT dependencies that make them more prone to additional security risks (perpetuated by deficiencies in system configurations, network design, software and platform vulnerabilities or lack of standards and policies). Hence, the use of SIS in the energy sector brings into question societal norms around competing priorities and around the deliberation processes for resolving conflicts and reaching consensus.

⁴⁷ Prosumer: "A prosumer is a person who consumes and produces a product. It is derived from "prosumption", a dot-com era business term meaning "production by consumers". These terms were coined in 1980 by American futurist Alvin Toffler, and were widely used by many technology writers of the time. Today it generally refers to a person using commons-based peer production." Source: Wikipedia: <https://en.wikipedia.org/wiki/Prosumer>

This section explores the ethical tensions related to the smart grid. Section 2.1 refers to ethical issues arising from the impact of smart grids on people's health. Section 2.2 deals with implications around privacy and industry practices around eliciting informed consent. Section 2.3 deals with cybersecurity risks threatening energy security.

2.1 Health and Safety: Does the smart grid make us unhealthy?

The wireless communication between smart appliances and the smart grid raises health and safety concerns relating to radio frequency radiation and its possible carcinogenic effects. Similar concerns are associated with cell phone usage. Research conducted by the Electric Power Research Institute on the health implication of the radio-frequency exposure of smart grids indicated that levels fall within acceptable thresholds as defined by the Federal Communications Commission (FCC) for the general public. Yet, adverse public perceptions persist. This has led to various levels of resistance and disputes. For example, in California, citizens and municipalities have resisted the rollout of smart meters, taking the case to the Federal court. The matter also remains open for debate by the International Agency for Research on Cancer (IARC, 2011). While the case was recently resolved in court, negative perceptions about potential health risks still persist (Weaver, 2018).

2.2. Privacy and Informed Consent: Does the smart grid give away household privacy?

Privacy concerns relate to the granularity of electricity consumption data that can be collected about a household and the intimate lifestyle information that can be inferred from it. For instance, smart meters can tell when someone is at home, whether they are cooking, taking a shower, or watching TV based on the monitoring the energy consumptions patterns (loads) of such appliances. Customers in general are uncomfortable with commercial organisations, including utilities, possessing such fine-level information (Gray, 2018). Some people also object to the mandate of being told to have a smart meter installed, unaware of how this decision was made and who were involved in this decision. Objections are then related to trust and transparency (Gray, 2018, Knapman, 2018). To mitigate such concerns, and in response to the General Data Protection Regulation (GDPR), utilities have embarked on educating customers regarding their privacy policies, the reasons behind data collection and sharing, accessing of data, and consumer rights.

Ofgem, the government regulator for gas and electricity markets in Great Britain for example, informs citizens of their rights and suggests that energy suppliers and network companies access smart meter data no more than once every 30 minutes to ensure accurate billing, carry out other essential tasks and share data (with customer consent) with third parties to offer them new products/services, such as dynamic billing options (see Smart Meter Your Rights at Ofgem.gov.uk). Yet, the British Chartered Trading Standards Institute (CTSI) have, however, received complaints from citizens about being misinformed and pressured to install smart meters, potentially breaching Consumer Protection Regulations and raising doubts about the industry's overall ethical code (Knapman, 2018).

New market players such as aggregators and storage operators are expected to offer dynamic consumption advice as a service to residential customers, contingent upon customers' consent to share their household consumption data. The company Efficiency 2.0, for example, delivers energy efficiency via customer engagement programmes, combining personalised technology portfolios and energy conservation actions with rewards and loyalty incentives to optimize energy savings⁴⁸. This raises the question as to who will be able to afford such services and at what cost. Given the high cost of energy as a percentage of discretionary income for poorer families, it also raises the question as to whether poorer families can afford to opt out from giving their consent if this is the only way to get cheaper energy, or will they be indirectly coerced into it? Furthermore, those who live in e.g. government-assisted accommodation where electricity is paid by the state or are occupants in shared private housing where the landlord controls the energy supply may not be given the option to consent individually.

2.3. Cyber-risks and Security: Do we jeopardise energy security?

Cyber-attacks on the smart grid can do significant damage, yet are still inadequately addressed, due to their low probability of occurrence (Eder-Neuhauser, et. al., 2017). Using coordinated, distributed resources, cyber-attacks could potentially target sufficient critical power control equipment simultaneously to originate cascading effects and eventually cause the system to collapse. This would not only be harmful to system integrity but also poses huge risks to human safety. The use of sensors and IoT networks opens up the energy grid to cyber-attacks that can cause disruption to energy distribution flows and even to the distribution infrastructure itself. As energy is fundamental for all aspects of modern living (from cooking to heating to telecoms), such disruptions can directly affect people's wellbeing.

To date, cyber-attacks on the energy grid have been sparse but raise significant concerns. In 2015 and again in 2016, hackers launched a cyber-attack on West Ukraine's power grid (Cherepanov, 2016). The Industroyer malware hijacked standardised industrial communication protocols, which are used in most critical infrastructure systems, to take direct control of electricity substation switches and circuit breakers to cut electricity in 250,000 households in Western Ukraine for several hours (Cherepanov and Lipovsky, 2017). Lying dormant until instructed otherwise, malware can be reactivated remotely to overwrite documents with random data or make the operating system unbootable. Cyberattacks on the energy grid have knock-on economic implications for citizens at a national level, and have cost the UK 545 million euro in losses alone, while global losses were estimated to be 1.69 billion euro in 2018 (Tofan et. al, 2016).

⁴⁸ Interestingly, the company was acquired and is not part of C3 platform, now offering behavioural and AI data analytics platforms for smart grids a platforms source <https://www.greentechmedia.com/articles/read/c3-acquires-efficiency-2-0#gs.v0jhVeYy>

2.4. Affordability and energy equity⁴⁹: A new criteria to set society apart

One of the key drivers for the smartification⁵⁰ of energy grids is to create energy abundance, or at least sufficiency, without the need for costly infrastructure investments, in order to maintain energy affordability for all (Ricci, et. al, 2012). The introduction of smart grids and active demand systems that monitor and incentivise alternative energy consumption habits can enable dynamic consumption of energy by enabling customers to shift their consumption to take advantage of dynamic pricing (ibid.).

Industrial and commercial organisations have experts who work on optimising energy requirements for their organisations. Citizens, however, lack the expertise, drive and flexibility to change their lifestyles according to dynamic pricing. The same holds for most SMEs and their energy consumption patterns (Faruqui, 2010). Energy aggregators and storage operators are expected to offer alternative services to facilitate dynamic consumption and manage the energy production of individual or community owned renewables. Nevertheless, smart energy systems will pose energy equity dilemmas around energy justice. For example, while the cost of the energy grid is funded via taxation and hence shared between citizens, the benefits from transition to smart grids are not equally shared. Affluent consumers (e.g. those who can afford electric cars or to invest in photovoltaic energy production) will reap the benefits of smart grids earlier and to a larger extent. Smart grids also raise questions about the potential of algorithmic bias in managing energy distribution. For example, how can we ensure that energy distribution algorithms will not be designed to favour charging an affluent person's electric car over the washing machine of a poorer family?

While smart grids are seen as one of the solutions to effecting energy justice or equity, what they in fact try to achieve is energy abundance so that there is enough supply to satisfy the disproportionate increases in energy demand (Sovakool and Dworkin, 2015). One could argue that via dynamic pricing, such technologies promote social engineering of the energy consumption patterns of large sections of the population for whom spending on energy consumption is a considerable part of their discretionary income, to support the ever-expanding list of electronic gadgets and (soon) electric vehicles available to the more affluent members of society (McCauley, et. al. 2019). Poorer socio-economic strata would be the most motivated to save on their energy costs but might find it difficult to benefit from dynamic pricing as their energy use is frugal to begin with. There is also a concern that dynamic pricing will leave consumers who are unable to shift their energy consumption worse off, as companies will try to 'penalise' energy use during peak times by raising prices (Faruqui, 2010).

2.5. Sustainability: Doing our bit for climate change

Smart grids are part of the EU's green energy strategy to tackle CO² emissions and climate change, in cost efficient ways. The more accurate and real-time the modelling that matches energy production with consumption can be, the more responsive the grid will be in managing electricity flows. Hence,

⁴⁹ Energy equity: An index that evaluates the accessibility and affordability of energy within a country or region, and one of the 3 core dimensions of the Energy Trilemma (Source: <https://www.worldenergy.org/wp-content/uploads/2017/11/World-Energy-Trilemma-2017-Full-report-WEA.pdf>)

⁵⁰ smartification (noun) : The process of transforming negative behavior into a smart personality.[from the root word smart] (Source: http://nws.merriam-webster.com/opa/opa_dictionary/newword_display_alpha.php?letter=Sm&last=20)

the more reliably renewables can be incorporated into the energy production mix. The transition to sustainable energy resources is key part of the climate change agenda and closely linked to issues of intergenerational justice. Another key contribution of smart grids towards the EU's sustainability goals is the transition of transportation systems from fossil-fuels to electric. While this will exponentially increase the demand for electricity over the coming years, it enables greater freedom as to which sources this electricity will come from. On the other hand, smart meters and SIS technologies come at an energy cost, as they themselves use electricity to function. Hence, they contribute to a country's overall energy consumption by the public sector as they become operational part of the energy distribution network, a critical infrastructure funded by taxation.

3. Liander: The Case of a Large Distribution System Operator using SIS in Smart Grids

This section will focus on a specific company, Liander. Liander is a DSO and as such responsible for introducing smart grid technologies (including smart meters) in the geographical areas of the Netherlands where it operates. According to Foss Ballo (2015), in the Netherlands the introduction of smart meters was met with resistance or indifference by the public for two key reasons: (i) unresolved privacy issues and (ii) lack of transparency, since decision-making about this policy happened 'behind closed doors'.

Market dynamics and their impact on progress and implementation were also explored. DSOs are transitioning from market facilitators to energy platforms with multiple providers, both traditional and innovative, relying on the customer insights of DSOs. This has created rivalry within the sector and a lack of clarity between energy players.

The aim of this section is to understand the company's perspective on the ethical issues arising from use of SIS by the organisation and by the sector overall. The section is informed by background research on the company's use of SIS technology, and interviews with Liander staff members on their experiences and use of SIS technologies and their views on the current and anticipated ethical issues pertaining to the use of SIS by both the company and the energy sector more generally.

3.1. Description of Liander

Liander is a typical Distribution System Operator (DSO) operating in the Netherlands. It manages the networks that transport electricity and gas from energy producers to customers. The company was founded in 2000 under the name N.V. Continuon Netbeheer and changed its name to Liander N.V. in December, 2008. It is based in Arnhem and is part of the ALiander N.V. group. There are three DSOs in the Netherlands, each servicing a different geographical area. Liander services 3.3 million households in the middle band of the Netherlands in the provinces of Gelderland and Noord-Holland, and parts of Flevoland, Friesland and Zuid-Holland. Much like other DSOs, it is publicly funded, and is expected to maintain its financial independence from its parent company (Alliander) to ensure that it provides a level ground for all utilities relying on its distribution network.

According to its website, “Liander is implementing Smart Grids to create an intelligent electricity supply system: substations and mid-voltage units are equipped with ICT and sensor technology to make the network intelligent, while also raising its capacity from 10 kV to 20 kV.”⁵¹ This is in response to the environmental sensibilities of modern society around energy use and the need to detach from fossil fuels which will become increasingly scarce and expensive. As part of that, the parent company ALiander has invested in a LiveLab to bring together managers, engineers and procurement staff to experiment with new technologies, equipment and processes that can improve the management and maintenance of energy networks.

Liander is tasked by the Dutch government to install smart meters for at least 80% of their customer base by 2020. To date, around 60% of its customer base has adopted smart meters. There is hence an urgency to reach out to another 20% of the market by 2020. Installation of smart meters is considered Phase I of the Energy Transition Plan, where meters are mainly used to raise customers insights into their own energy usage and drive behavioural changes or purchasing decisions that can lead to lower energy consumption. Phase II of the Energy Transition plan, to commence after 2020, is the use of smart meters as a means to support the smarter management of grids and enable innovation in the energy ecosystem. For example, this could enable energy suppliers to develop and deliver new services and flexible tariffs for electricity; allow for more than one electricity provider to serve the same household; and facilitate transactions in renewable microgrids with the main grid.

Liander is involved in various pilot initiatives to experiment with smart grid technologies. For example, it has been involved in microgrids projects with citizens and aggregators, such as citizens investing together in generating energy via solar panels, and in collective purchasing of energy facilitated by aggregators (companies which specialize in the automation of high and middle voltage stations), as well as the production of smart sensors. ALiander has also created LiveLab, a mid-voltage network in Bommelerwaard dedicated to live testing of innovative technologies, equipment and processes, with collaboration from asset managers, network managers, engineers and procurement staff (see Figure 5 below).

⁵¹ <https://www.aliander.com/en/innovation/our-innovations>



FIGURE 5: LIVELAB ALLIANDER (SOURCE: [HTTPS://WWW.ALIANDER.COM/EN/INNOVATION/OUR-INNOVATIONS](https://www.aliander.com/en/innovation/our-innovations))

Joint interviews were conducted with members of the Data Protection team within Liander. While Data Protection Officers (DPOs) are formally an independent role, the DPO sits hierarchically within the Customer Relations department. The DPO team is responsible for ensuring the company's compliance with GDPR and enabling the organisation to utilise and make data available to private organisations in order to facilitate the development of utility services to customers. GDPR is seen by the interviewees as a factor halting progress towards the further adoption of technology by new customers by raising suspicion about corporations' use of smart meter data. Hence, Liander has been proactive in coordinating Liander's effort towards lifting barriers to smart meter adoption and utilisation of smart meter data and advising on how to use personal data within the limits of the law.

3.2. Description of SIS technologies used in Liander

Liander does not currently use AI as a means to run and manage energy distribution, as envisioned by industry and academic literature, and makes limited use of existing smart meter data. Smart meter data collection and analysis is a prerequisite for the development and testing of an operating model that could utilise AI to run a smart grid autonomously or semi-autonomously, and hence the installation of smart meters to the majority of the customer basis is a first step in this direction. Yet, while data from smart meters are getting collected by smart meters in approx. 60% of Liander's customer base, they remain mostly unused (see more on this in section 3.3 below) primarily due to lack of clarity in the implementation of privacy laws. Despite these tensions, different types of data can legitimately be collected via smart meters:

- a) Consumption data collected in 15-minute intervals and currently stored within the smart meter.

- b) Power quality voltage data are not related to energy consumption behaviour. Power quality data related to voltage spikes and dips and is not made available through smart meters. In addition, such data cannot be requested by energy suppliers or third parties.
- c) Power quality energy data is related to energy consumption behaviours. This type of data is treated the same as consumption data. Power quality energy data is not made available via the smart meters and cannot be requested by energy suppliers or third parties.
- d) Pinging the meter, to ensure control of and access to the meter by Liander.
- e) Event data, i.e. status information (indicators, alarms and error messages) from the meter

Once the legal issues around the use of data get clarified, data from smart meters can be used for the management of the energy grid and, in the future, could also support the provision of personalised services at household level. The granularity of data collection and analysis depends on the purpose of data analytics. Usually, in order to monitor grid performance the company requires aggregated data for smart meters connected to the same energy line, which can involve several hundred meters. When a household experiences a problem with their electricity supply, a specific smart meter needs to be engaged with to diagnose energy leakages. Energy leakages can occur due to a fault in the energy distribution network, or due to energy theft, resulting in unaccounted energy consumption being compensated by the DSO and hence by tax payers money. The company aspires to use smart meter data for various purposes such as:

- Error, failure and hazard detection, analysis, and prediction
- Power quality monitoring to ensure quality standards set out by law
- Network capacity planning to inform investments
- Visualisation of performance and adherence to quality standards
- Status and events recording

To monitor the functioning of the energy grid and detect any malfunction, one needs to combine smart meter readings of events and check the accessibility of the meters and the power quality voltage. This is in line with the company's legal obligations and no analysis of energy consumption data is required. Malfunctions of the energy grid are automatically linked to a compensation fee to the customer, hence it is important to accurately record the duration of the malfunction. To do so, a post-hoc analysis is performed by reading smart meter data on power quality.

Consumption data are used for predicting and projecting energy demand and detecting fraud. Consumption data, along with power quality, can be read for a specific period in order to monitor the capacity of the network for the purposes of planning, so that potential bottlenecks can be solved or limited. Consumption data can indicate cases of energy theft (as in the case of drug farms, or vacant property squatting, for example) or loss of energy due to technical issues. According to Liander's drafted code of conduct, personal data can be used when:

- (a) the data subject has given consent for the processing of personal information for one or more specific purposes;
- (b) The processing of personal data is necessary for the execution of an agreement in which the Party concerned is involved, or to take measures at the request of the person concerned before the conclusion of an agreement;

- (c) The processing of personal data is necessary in order to comply with a legal obligation which rests on the system operator;
- (d) The processing of personal data is necessary to protect the vital interests of the person concerned or of another natural person;
- (e) The processing of personal data is necessary for the performance of a task of general interest or of a task within the framework of the exercise of the public authority entrusted to the processor responsible;
- (f) The processing of personal data is necessary for the protection of the legitimate interests of the network operator or of a third party, except where the interests or fundamental rights and freedoms of the person concerned which protect Personal data require more weight than those interests, especially when the person concerned is a child.

3.3 The effectiveness of using SIS for Liander

Both interviewees agreed that the use of AI for Liander is at an early stage and that moving towards the development of autonomous grid management systems will require the majority of consumers to install smart meters, and legal and regulatory barriers to be lifted. Currently, smart sensors and Big Data analytics are successfully used for post-hoc analysis of energy disturbances to create models that can predict future disturbances. SIS allow the organisation to quickly locate technical issues within the grid and respond swiftly to manage energy disturbances. This also allows for accurate accounting of energy outages to provide customer compensation. Smart meter data is also used to locate energy loss and understand the reasons for the energy loss due to theft, unaccountability of energy usage and/or inaccurate information.

Analysis of smart meter data from already installed smart meters is ridden with difficulties due to GDPR and its interpretation. Big Data analytics are used ad hoc, on a case-by-case basis, following the consent of affected customers and/or obtaining the approval of the Dutch Personal Data Authority, both of which cause delays and require a clear and detailed justification. The interviewees said that the reason for these difficulties is that the authority does not understand the business and its applications. They just check the data analytics processes against the letter of the law, the implementation of which can be unclear. This, coupled with negative publicity about the potential misuse of smart meter data, deters the authority from approving something that society might have a problem with afterwards and setting precedence that would be difficult to undo.

To tackle privacy concerns, Liander has come together with the other two DSOs serving the Netherlands to develop a code of conduct for the industry in terms of dealing with smart meter data. This was submitted to the Personal Data Authority for approval in March 2018, prior to GDPR becoming effective. The code of conduct seeks to bring some clarity around the implementation of GDPR in the sector and its agreement with the Personal Data Authority in order to provide some peace of mind around legal implications. This was to clarify the authority's position on "processing of meter data by or on behalf of the System Operator for its statutory duties" and "for market facilitation". It also clarifies the extent to which smart meters are considered to process personal data (article 29, GDPR) and whether data contain any special categories of personal data mentioned in article 9 of the GDPR. The purpose of this code of conduct (Unpublished, 2018) is:

- a) to establish rules for network operators to process meter data from remotely readable meters;
- b) to provide information to data subjects whose meter information is processed by grid operators in relation to the distance readable meter;
- c) to contribute to the transparency of how grid operators deal with energy suppliers and third parties for processing measurement data of remotely readable meter; and
- (a) to contribute to transparency with regard to the processing of personal data collected by remotely readable meters.

The code of conduct has been returned with comments and recommendations and is soon to be revised.

4. Liander: Ethical issues from SIS Technology

This section aims to identify which ethical issues have arisen for Liander, whether there are policies and procedures in place, and what their protocol is for addressing these concerns. This section relies not only on the interviews conducted with representatives of Liander, but also on desktop research on the company's website and related material from the organisation.

The following ethical concerns are listed: 4.1 Privacy and informed consent; 4.2 Security of the smart grid; 4.3 Data stewardship and market dynamics; 4.4 Prioritization of energy distribution and energy justice.

4.1 Privacy and informed consent

The company sees smart meter acceptance levels dropping due to ethical tensions in the interaction between customers and organisations. According to the interviewees, the current barrage of GDPR articles in the media has raised the public's privacy concerns and suspicion towards the company. The situation is exacerbated by the fact that it has been difficult to obtain certification by Dutch Personal Data Authority to demonstrate to the public that the organisation follows acceptable data management practices. Privacy concerns relate primarily (but not solely) to energy consumption data collected by smart meters from which inferences about behaviour can be drawn, due to the granularity of electricity consumption data that can be collected about a household and the intimate lifestyle information that can be inferred from it.

To date, aggregated consumption data are used for predicting and projecting energy demand, by exception, i.e. to check electricity consumption in vacant properties or periodically to detect fraud (i.e. energy theft) or technical issues (i.e. energy leaks). Such tapping into energy consumption data may be negotiable with the public through a more coherent discussion on the risks and benefits that are required for people to understand the implications, and design organisational processes for seeking and eliciting consumer consent on specific use cases. Privacy concerns may be more sinister, however, as DSOs move towards Phase II of the Energy Transition Plan, that will require real-time monitoring of all smart meters for market facilitation and the development of AI systems for monitoring, diagnosing and operating the smart grid. In addition, there is undoubtedly a high tension between consumer

privacy and the protection of the smart energy grid. To protect the energy grid, insight into the energy flows is required, but it can only be appropriately visualised by reading consumer data from all individual smart meters collectively in real time.

The company's frustration with GDPR can be explained by the sector's failure to resolve competing demands facing DSOs and the lack of a cohesive strategy for doing so, as well as Liander's inability to tackle the distrust facing utilities overall. On the one hand, the target for introducing smart meters by 2020 to 80% of the customer basis did not account for GDPR and was not reviewed after the effects of GDPR on public perception became apparent. The company is, thus left with the obligation to adhere to a goal while the conditions have changed, with little support or guidance from relevant authorities. For example, the Personal Data Authority was unable to provide guidance on how the company can use smart data within the limits of the new law and unwilling to ratify any proposals put forward in time to facilitate progress. On the other hand, the company has limited capacity, capability and experience in engaging the sector and the public in direct deliberation processes, and perhaps even feels constrained by industry norms to do so in order to explore acceptable ways forward. Admittedly, there will be ethical issues arising from the constant surveillance of energy consumption in Phase II of the energy transition, and there is a lack of deliberation of how these issues will be resolved, or institutional and political commitments on how they will be mitigated. Phase II is often discussed in relation to the ability of the organisation to incentivise behavioural change via economic benefits, rather than the ethical and social implications of dynamic pricing with respect to energy equity or energy justice.

4.2 Security of the smart grid

The ultimate threat to smart grids is the possibility of disruption in energy transmission, which can affect energy security and effectively all fundamental aspects of life – including heating, cooking, communication, transportation, healthcare, commerce, and many more. According to Liander, as the grid will ultimately rely only on the data from sensors and their automated processing, the impact of disruption may be high and the possibility of it going unnoticed for long periods will be longer. On the other hand, insights into the energy flows and monitoring usage data from all individual smart meters collectively and in real-time will help to detect inconsistencies faster. In addition, analytics can help to resolve disruptions faster because energy flows can be redirected in near real-time.

Cyberattacks mainly only disrupt the function of the grid, but balance of trade between energy providers, DSOs, energy suppliers and customers. Manipulating for example the meters may result in miscalculation of energy flows. By law, unaccounted consumption of energy is compensated by publicly funded DSOs, and this can result in losses that will be compensated by the government via taxation. Hence, it is important that accurate accounting of energy flows is maintained.

Dealing with cybersecurity issues arising from the complexity of the decentralised architecture and the digitisation of multiple points in the grid, all of which can be individually attacked to trigger a cascading response that may lead to energy disruption or failure of the infrastructure (e.g., blowing the fuses of energy exchanges). As it will be impossible to safeguard the infrastructure entirely, the emphasis is shifting towards containing possible contagion and its cascading effects. Interestingly, reliance on standardized technologies and technology vendors may increase risks, as the same bugs

can be exploited for bigger impact. Hence, avoiding long-term contractual agreement with supplies is paramount. Changing vendors quickly to avoid viruses exploiting common vendor vulnerabilities can be a mitigation tactic to avoid contamination.

This will require systemic coordination by all parties in the energy sector – suppliers, DSOs, and energy consumers. DSOs are joint owners of EDSN (Energy Data Services Netherlands), the entity with the task of distributing energy data to all players in the energy sector. While Liander, as a DSO and grid operator, must ensure that energy transport is fulfilled and that the energy balance in the grid is always maintained, other key players have roles to play. For example, the government must draft relevant laws and regulations and ensure compliance with these regulations and clarify their implementation. Solutions on how to respond to these legal requirements should be accepted by the energy ecosystem to avoid each player seeking to protect their own interests and ensure that the implementation of legislation does not leave room for internal politics that block such solutions. Specific cyber threats and implications for cybersecurity are difficult to predict in order to make provisions into the system design and the institutional environment, yet a concerted effort to put together a pan-European cybersecurity framework has recently been formed by means of a Cybersecurity Act, which includes an EU Cybersecurity that will affect the management of critical infrastructures and related equipment as well as consumer products (EC, 2017).

4.3 Other issues

Data stewardship and market dynamics: Liander sees the role of the organisation developing as one of energy data stewardship, which manages the “Data-Driven Grid”. In a digital world where information is power, smart meter stewardship is changing industry dynamics and has created conflicts within the sector, halting progress towards energy transition. Energy consumption data is particularly crucial for energy service providers who traditionally had access to both customer information and customers. With DSOs having direct access to and responsibility for customer data, customer insights become the privilege of DSOs. Hence their role is growing more prominent within the market and will be even more so in phase II of the Energy Transition.

Prioritization of energy distribution and energy justice: While the goal of smart grids is to avoid energy scarcity, Liander recognises that balancing energy provision between competing priorities will become a point of political and societal debate that will touch company policies and priorities in Phase II of the Energy Transition. For example, how should AI be able to distinguish and prioritise between domestic uses, industrial uses and electric car uses, particularly in cases of energy scarcity? These concerns relate primarily to issues of distributive justice. Transparency in energy distribution and the use of “explainable AI”⁵² that can provide evidence of energy distribution choices and inform social debates is likely to become pertinent in the future and is fundamental for establishing the social capital and procedural justice that can springboard technology acceptance.

⁵² https://en.wikipedia.org/wiki/Explainable_Artificial_Intelligence

4.4 Mechanisms for addressing ethical issues

The company recognises that engagement of the public has been relatively low and localised, a step forward from typical old-fashioned management strategies, particularly in traditional services such as the utility sector. They are actively looking to set up a programme to engage customers and relevant NGOs more substantively.

Liander has been instrumental in aiming to address issues of social acceptability of smart meters and address the privacy issues. For example, it has coordinated the development of a code of conduct to address public concerns and sought to have it approved by the Personal Data Authority to ensure that the company remains within the law and attracts public trust. Liander is also keen to develop a scheme to engage the public in dialogue to address their concerns.

5. Conclusion

This case study contributes to knowledge regarding Big Data/AI ethics, and to empirical research on the implementation of SIS technologies in the energy sector.

Ethical issues are delaying the integration and use of SIS technologies in energy grids. This case study explores the ethical issues arising from its implementation the purpose of using SIS in the energy sector. The two interviews with Liander employees offered an understanding of the current state of the use of SIS in the energy sector and discussed the practical, industry, and ethical issues arising from the use of SIS in this sector.

The critical ethical issue resulting from the use of SIS by energy utilities to date is privacy. Privacy directly relates to household energy consumption data currently collected and stored in smart meters. Privacy issues are seriously debated and are affecting the installation of smart meters in households in the Netherlands to the desired 80% level. Privacy concerns are thus presently a key barrier for the rollout of smart meters and their acceptance by the public. The following issues were also identified: security of the smart grid, changes in market dynamics, and energy justice. In addition to suspicion around the use of technology, there is suspicion about Liander as a company, its role and agendas, and the extent to which it operates in the public interest. The company has recognised the need for further engagement with the public and actively seeks solutions and recommendations to achieve this goal. During the interview, the idea of engaging them as members of the LiveLab to capture the concerns during the development of ideas and ensure that solutions are based on their values and privacy concerns. They can also engage the whole ecosystem in Future Search research to give customers an insider's view of industry developments and rationale and allow them to influence priorities and industry strategies. There is also the possibility to:

- I. undertake deep qualitative, ethnographic research with their most avid objectors to understand their underlying concerns and their relative importance;
- II. guarantee adherence and transparency of industry practices by allowing customer juries on their board and data management practices;

- III. co-opt other DSOs internationally in educating the public and co-develop a code of conduct in collaboration and even create a sectoral fund to employ an international legal firm to promote its progression with Personal Data Authorities (or their equivalent) in all European countries.

5.1. Implications of this Report

This report highlights the interplay between government policy, legal requirements, and industry dynamics with respect to the ethical issues arising from the use of SIS in the energy sector. While transition to smart grids is fundamental at a country our research highlights the inability of policy makers, industry players and legal authorities to engage the public in meaningful dialogue and align public and national interests around the energy transition. The document highlights the need for clarification in practice of privacy policies (particularly of GDPR) to lift concerns about the capability of organisations to remain within its boundaries without holding back progress.

5.2 Further Research

This report has implications for the further exploration of ethical issues in the use of SIS in the energy sector. While smart grid technologies are a relatively new phenomenon, piloting research needs to take place to understand how they change social life, interactions between people in a community, their values and local culture.

The report is also valuable in highlighting the state of affairs, highlighting gaps and providing direction towards future research into the topic for other DSOs and policy makers, and informing funding decisions and economic investments into smart grids to include further research.

6. References

Ballo-Foss, I. (2015). Imagining energy futures: Sociotechnical imaginaries of the future Smart Grid in Norway. *Energy Research & Social Science*, [online] 9, pp.9-20. Available at: https://ac.els-cdn.com/S2214629615300384/1-s2.0-S2214629615300384-main.pdf?_tid=a0793a08-5d01-46db-add0-1be97a108d21&acdnat=1539713779_a89a14c136f0aec5b771404bc5b191c9. [Accessed 25 Jan. 2019].

Cherepanov, A. and Cherepanov, A. (2016). *BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry*. [online] WeLiveSecurity. Available at: <https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/> [Accessed 25 Jan. 2019].

Cherepanov, A. and Cherepanov, A. (2017). *Industroyer: Biggest threat to industrial control systems since Stuxnet*. [online] WeLiveSecurity. Available at: <https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/> [Accessed 25 Jan. 2019].

EC (2014) COM(2014) 356 Benchmarking smart metering deployment in the EU-27 with a focus on electricity final

EC (2016) Transforming the European Energy System through Innovation: Integrated Strategic Energy Technology (SET) Plan Progress in 2016 (doi:10.2833/661954), Luxembourg: Publications Office of the European Union, 2016

EC, (2017). *State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks* Available at: http://europa.eu/rapid/press-release_IP-17-3193_en.htm [Accessed 25 Jan. 2019].

Faruqui, A. (2010) *The Ethics of Dynamic Pricing* Available at: http://gridsolar.com/smartgrid/docket2010-267/Attachment_11.pdf [Accessed 25 Jan. 2019].

Gray, J. (2019). *Pricing and trust: a utilities conundrum - Utility Week*. [online] Utility Week. Available at: <https://utilityweek.co.uk/pricing-trust-utilities-conundrum/> [Accessed 25 Jan. 2019].

IARC MONOGRAPHS 102 (2011) *Non-ionizing Radiation Part 2: Radiofrequency electromagnetic fields*. Available at: <https://monographs.iarc.fr/wp-content/uploads/2018/06/mono102.pdf>

IEA (2017) Digitization and Energy Available at: <https://www.iea.org/publications/freepublications/publication/DigitalizationandEnergy3.pdf> [Accessed 25 Jan. 2019].

Knapman, H. (2018). *Households pressured into getting smart meters*. [online] Available at: <https://www.moneywise.co.uk/news/2018-01-30/households-pressured-getting-smart-meters> [Accessed 25 Jan. 2019].

Liang, X. (2017). Emerging Power Quality Challenges Due to Integration of Renewable Energy Sources. *IEEE Transactions on Industry Applications*, [online] 53(2), pp.855-866. Available at: <https://ieeexplore.ieee.org/abstract/document/7738432>.

McCauley, D., Ramasar, V., Heffron, R., Sovacool, B., Mebratu, D. and Mundaca, L. (2019). Energy justice in the transition to low carbon energy systems: Exploring key themes in interdisciplinary research. *Applied Energy*, [online] 233-234, pp.916-921. Available at: <https://www.sciencedirect.com/science/article/pii/S0306261918315587#!>. [Accessed 25 Jan. 2019].

Rathi, A. (2017) *The UK's electrical grid is so overrun with renewable power, it may pay wind farms to stop producing it*. Available at: <https://qz.com/952827/the-uks-electrical-grid-is-so-overrun-with-renewable-power-it-may-pay-wind-farms-to-stop-producing-it/> [Accessed: 19 January, 2019]

Ricci, A., Faberi, S., Brizard, N., Bougnoux, G., Degel, M., Velte, D and Garcia, E. (2012): *Smart grids/Energy grids: The techno-scientific developments of smart grids and the related political, societal and economic implications*. Available at: [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/488797/IPOL-JOIN_ET\(2012\)488797_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/488797/IPOL-JOIN_ET(2012)488797_EN.pdf) [Accessed 25 Jan. 2019].

Rojin, R. K. (2013). A Review of View of Power Quality Problems and Solutions in Electrical Power System. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation*

Engineering. Available at: <http://www.rroij.com/open-access/a-review-of-power-qualityproblems-and-solutions-inelectrical-power-system.php?aid=42532> [Accessed 25 Jan. 2019].

Sovacool, B. and Dworkin, M. (2015). Energy justice: Conceptual insights and practical applications. *Applied Energy*, 142, pp.435-444.

TOFAN, D., NIKOLAKOPOULOS, T., DARRA, E. (2016) *ENISA: The cost of incidents affecting CII: Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII)* Available at: *The cost of incidents affecting CII*.pdf [Accessed 25 Jan. 2019].

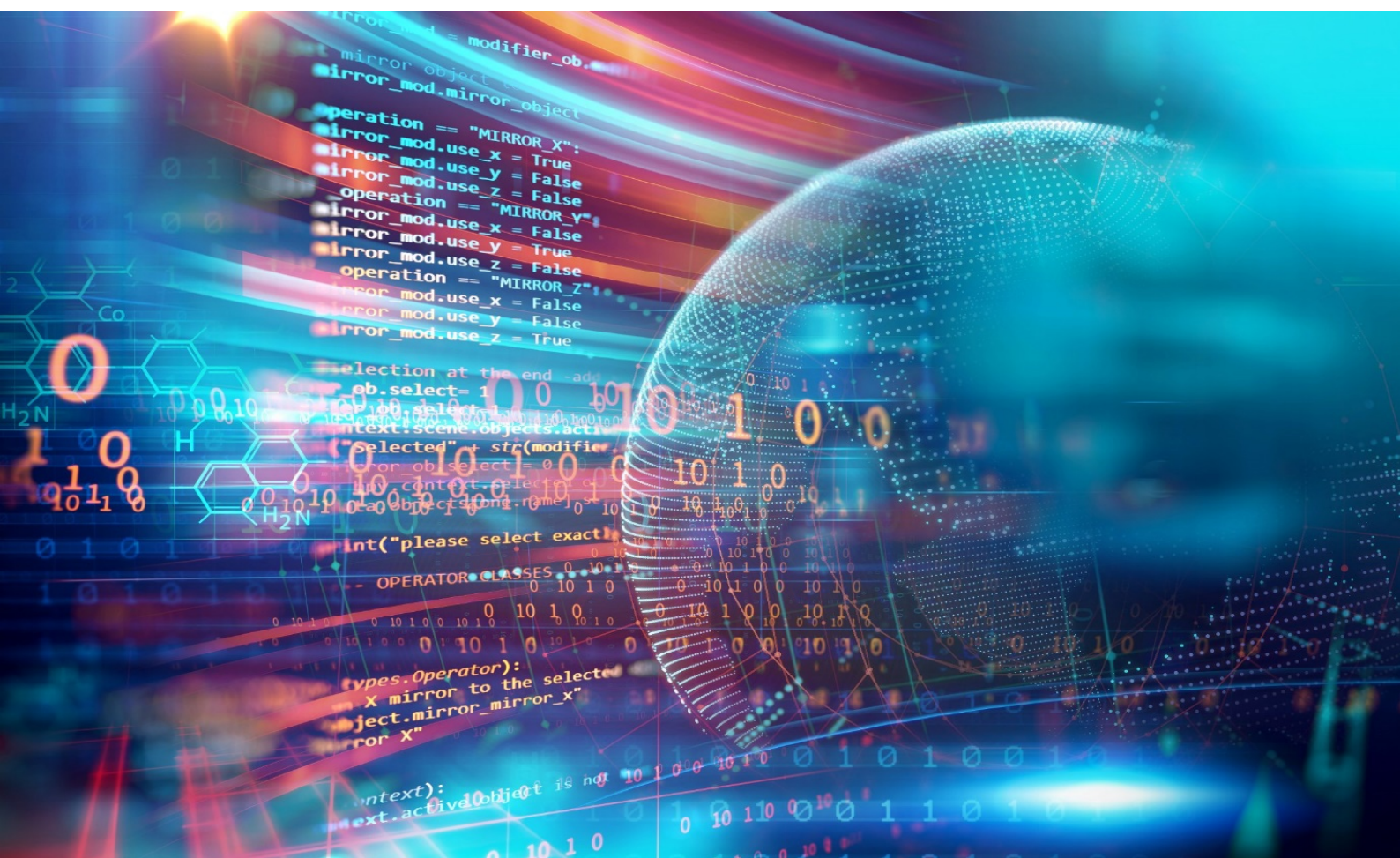
Weaver, K. T. (2018) *Federal Court Rules against Consumers on Smart Meters and Privacy Rights*. Available at: <https://smartgridawareness.org/2018/08/18/federal-court-rules-against-consumers-on-smart-meters/> [Accessed 25 Jan. 2019].

Weaver, K.T (2014) *Dutch case study: “smart” meter privacy invasions are unjustifiable in a democratic society* Available at: <https://takebackyourpower.net/smart-meter-privacy-invasions-are-unjustifiable-in-a-democratic-society/> [Accessed 25 Jan. 2019].

CS08 – Communications, Media and Entertainment



Case Study: Cybersecurity, Smart Information Systems and Ethics



This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641



Document Control

Deliverable	Deliverable 1.1.: Case Studies
WP/Task Related	WP 1: Representation and Visualisation
Delivery Date	31 January 2019
Dissemination Level	Public
Lead Partner	University of Twente
Contributors	Kevin Macnish, UT; Ana Fernandez, UT; Alexey Kirichenko, F-SEC
Reviewers	Mark Ryan, UT
Abstract	<p>This report provides an overview of the current implementation of SIS in the field of cybersecurity. It also identifies the positive and negative aspects of using SIS in cybersecurity, including ethical issues which could arise while using SIS in this area. One company working in the industry of telecommunications (Nokia) is analysed in this report. Further specific ethical issues that arise when using SIS technologies in Nokia are critically evaluated. Finally, conclusions are drawn on the case study and areas for improvement are suggested.</p>
Key Words	Cybersecurity, ethics, smart information systems, big data

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes
0.1	12/12/2018	Ana Fernandez	Kevin Macnish	First draft
0.2	17/12/2018	Kevin Macnish	Mark Ryan	Second draft
0.3	16/01/2019	Kevin Macnish	Mark Ryan	Revision
1.0	23/01/2019	Kevin Macnish	Mark Ryan	Revision

Contents

Executive Summary	226
Smart Information Systems in Cybersecurity: An Ethical Analysis	227
1.The use of Smart Information Systems in Cybersecurity	228
2. Literature Review - Ethical Issues of Using SIS in Cybersecurity	229
2.1 Informed Consent	229
2.2 Protection from Harm	229
2.3 Privacy and Control of Data	230
2.4 Vulnerabilities and disclosure	230
2.5 Competence of Research Ethics Committees	231
2.6 Security issues	231
2.7 Trust and transparency	231
2.8 Risk	233
2.9 Responsibility	233
2.10 Business interests and codes of conduct	233
3. The Case Study of a Cybersecurity company using SIS	234
3.1 Description of SIS technologies being used in Nokia	234
3.2 The effectiveness of using SIS by Nokia	236
4. Ethical Implications in Cybersecurity	236
4.1 Privacy	236
4.2 Internationalization, standardization and legal aspects	237
4.3 Monetization issues	238
4.4 Anomalies.....	239
4.5 Policy issues, awareness and knowledge.....	239
4.6 Security	240
4.7 Risk Assessment	240
4.8 Mechanisms to address ethical issues	241
5. Conclusion	241
5.1 Implications of this report.....	242
5.2 Future research.....	242
6. References	243

Executive Summary

This case study explores the principal ethical issues that occur in the use of Smart Information Systems (SIS) in cybersecurity, and offers suggestions as to how they might be addressed. This was carried out by studying key issues within a literature review and through an interview with three employees working at the telecommunications company Nokia. The aim of this case study is to identify which ethical issues arise from the use of SIS in cybersecurity, whether there are policies and procedures set in place for addressing these concerns in the company interviewed, and whether practitioners are facing additional issues not addressed in current literature.

The literature review highlighted a number of ethical issues. These included protection from harm, privacy and control of data, competence of research ethics committees, security issues, risk, business interests, codes of conduct and responsibilities issues. All of these were, to some extent, raised and discussed in the interview. The literature review also raised issues of vulnerabilities and disclosure, trust and transparency and informed consent, none of which was discussed in the interview. At the same time, the interview raised concerns regarding anomalies which are not discussed in the literature.

The case study hence highlights the ability of case studies to identify ethical issues not covered (or covered to an inadequate degree) in academic literature and yet which are facing practitioners in the industry of cybersecurity.

Smart Information Systems in Cybersecurity: An Ethical Analysis

Increasing numbers of items are becoming connected to the internet. Cisco, a global leader in information technology, networking and cybersecurity, estimates that more than 8.7 billion devices were connected to the internet by the end of 2012, a number that will likely rise to over 40 billion in 2020 (Singer and Friedman 2014). Cybersecurity has therefore become an important concern both publicly and privately. In the public sector, governments have created and enlarged cybersecurity divisions such as the US Cyber Command and the Chinese “Information Security Base”, whose mission is to provide security to critical national security assets (Singer and Friedman, 2014, p. 3).

In the private sphere, companies are struggling to keep up with the required need for security in the face of increasingly sophisticated attacks from a variety of sources. In 2017, there were “over 130 large-scale, targeted breaches [by hackers of computer networks] in the U.S.,” and “between January 1, 2005 and April 18, 2018 there have been 8,854 recorded breaches” (Sobers, 2018). Furthermore, cyberattacks affect not only the online world, but also lead to vulnerabilities in the physical world, particularly when an attack threatens industries such as healthcare, communications, energy, or military networks, putting large swathes of society at risk. Indeed, it has been argued that some cyberattacks could constitute legitimate grounds for declarations of (physical) war (Smith, 2018).

Cybersecurity is therefore a complex and multi-disciplinary issue. Security has been defined in the international relations and security studies spheres both as “the absence of threats to acquired values” (Wolfers, 1952) and “the “absence of harm to acquired values” (Baldwin, 1997). Within the profession, cybersecurity is more commonly defined in terms of confidentiality, integrity and availability of information (Lundgren and Möller, 2017). A 2014 literature review on the meanings attributed to cybersecurity has led to the broader definition of cybersecurity as “the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems” (Craig et al., 2014, p. 13).

Cybersecurity therefore can be seen to encompass property rights of ownership of networks that could come under attack, as well as other concerns attributed with these, such as issues of access, extraction, contribution, removal, management, exclusion, and alienation (Hess and Ostrom, 2007). Hence cybersecurity fulfils a similar role to physical security in protecting property from some level of intrusion. Craig et al also argue that cybersecurity refers not only to a technical domain, but also that the values underlying that domain should be included in the description of cybersecurity (2014, p. 17). Seen this way, ethical issues and values form a bedrock to cybersecurity research as identifying the values which cybersecurity seeks to protect.

The case study is divided into four main sections. Sections 1 and 2 focus on the literature review: section 1 reviews the technical aspects of cybersecurity, while section 2 presents a literature review of academic articles concerning ethical issues in cybersecurity. Section 3 focuses on the practice of cybersecurity research through an interview conducted with three employees at Nokia. Finally, section 4 critically evaluates ethical issues that have arisen in the use of SIS technologies in cybersecurity.

1.The use of Smart Information Systems in Cybersecurity

The introduction of big data and artificial intelligence (Smart Information Systems, or SIS) in cybersecurity is still in its early phase. Currently there is comparatively little work carried out on cybersecurity using SIS for several reasons. These include the remarkable diversity of cyberattacks (e.g. different approaches to hacking systems and introducing malware), the danger of false positives and false negatives, and the relatively low intelligence of existing SIS.

Taking these in turn, the diversity of attacks, both in the source of the attack, the focus of the attack and the motivation of the attack is significant. Attacks can be launched from outside an organization (e.g. from a hacking collective, such as Anonymous) or from an insider (e.g. a disaffected employee looking to damage a system). They may come from a single source, typically masked through using the dark net, or from a source who has engaged in a number of “hops” (moving from one computer on a network to another, thus masking the original source) such that the originator could appear to be in a hospital or in a military base. If the attack appears to come from a military base this might encourage the attacked party to “hack back”. However, if the military base were an artificial screen presented in front of a hospital, the reverse hack could bring down that hospital’s computer networks. The focus of the attack could be on imitating a user or systems administrator (local IT expert) or on exploiting a security flaw in unpatched code (programming in a network that has a flaw which has not yet been fixed, also known as a zero-day exploit). The motivation of the attack can range from state security and intelligence gathering (e.g. US Intelligence spying on Chinese military installations), to financial incentives through blackmail (e.g. encrypting a company’s files and agreeing to decrypt them only when the company has paid the hacker a certain sum of money). This diversity means that it is extremely difficult to develop a SIS that will effectively recognize an attack for what it is.

Secondly, the danger of false positives and false negatives is significant in light of the difficulty of recognizing an attack. If an attack is not recognized by a SIS then as a false negative it may be successful. This is particularly the case if security personnel have come to place undue trust in the automation and so do not provide quality assurance of the SIS, which is known as “automation bias” (Bainbridge, 1983; Goddard et al., 2012). By contrast, the SIS could be so cautious that it may lead to an excessive number of false positives in which a legitimate interaction is falsely labelled an attack and not permitted to continue. This leads to frustration and could entail the eventual disabling of the SIS (Tucker, 2018).

Thirdly, and despite some hype in the media, SIS are still at a relatively unintelligent stage of development. Computer vision systems designed to identify people loitering, for example, recognize that a person has not left a circle with radius x in y number of seconds, but cannot determine why the person is there or what their intent may be. As such, the inability to determine intentions from actions renders automated systems relatively impotent.

Despite these concerns, there are some potential grounds for use of SIS in cybersecurity. The most effective is in scanning systems for known attacks, or known abnormal patterns of behaviour that have a very high likelihood of being an attack. When coupled with a human operator to scan any alerts and so determine whether to take action, the combined human-machine security system can

prove to be effective, albeit still facing the above problems of automation bias and excessive false positives (Macnish, 2012).

2. Literature Review - Ethical Issues of Using SIS in Cybersecurity

In this section we will conduct a literature review of the most fundamental ethical issues in cybersecurity that are being proposed in the academic environment. Our goal is to compare them with the interview that has been conducted in the telecommunications company Nokia, in order to give an overview on the ethical issues in cybersecurity.

The literature review was carried out through a combination of online search using generic engines such as Google and Google Scholar and discipline-specific search engines on websites such as PhilPapers.org and the Philosophers' Index. Selected papers were then read and, where appropriate, the bibliographic references were used to locate further literature. Generic search on Google also provided links to trade publications and websites that were a further source of background information.

The ethical issues to arise from the literature review were informed consent; protection from harm; privacy and control of data; vulnerabilities and disclosure; competence of research ethics committees; security issues; trust and transparency; risk; responsibility; and business interests and codes of conduct.

2.1 Informed Consent

Acquiring informed consent is an important activity for cybersecurity, and one that has been at the heart of research ethics and practice for decades (Johnson et al., 2012; Miller and Wertheimer, 2009). Consent is variously valued as the respect for autonomy (Beauchamp, 2009) or the minimization of harm (Manson and O'Neill, 2007). However, within global cybersecurity a number of complicating issues arise, such as the complexity of informing users about detailed technical aspects in order to provide necessary information, as well as language barriers (Burnett and Feamster, 2015). This, though, is the case for many other areas of research such as medical or social sciences, and the scripts need not be different in cybersecurity (Macnish and van der Ham, 2019).

Nonetheless, challenges of complexity, and of conveying that complexity in a manner that is sufficiently informative for a non-expert to make a decision, remain. Wolter Pieters notes that information provision does not correspond merely to the amount of information communicated, but how it is presented, and that the type of information given is justified and appropriate. "One cannot speak about informed consent if one gives too little information, but one cannot speak about informed consent either if one gives too much. Indeed, giving too much information might lead to uninformed dissent, as distrust is invited by superfluous information" (Pieters, 2011, p. 61).

2.2 Protection from Harm

Cybersecurity has the potential to cause harm to its users, even when that harm is not intended. Concerns exist regarding the disclosure of vulnerabilities (such as a flaw in a security program which would allow for a hacker to break into the network with relative ease), for example, such as whether

they should be disclosed publicly once a company has failed to address them. If not then the vulnerability entails that a person may be at risk of attack, which is particularly concerning if the device at risk is medical in nature, such as a pacemaker (Nichols, 2016; Spring, 2016). However, disclosure could bring the vulnerability to the awareness of potential attackers who had not considered it previously.

2.3 Privacy and Control of Data

Privacy is a central issue in cybersecurity, as increasing amounts of personal data are gathered and stored in the cloud. Furthermore, these data can be highly sensitive, such as health or bank records (Manjikian, 2017, pp. 81–112). While the data at risk from attack is private, in order to identify an attack, particularly when SIS are involved, an effective cybersecurity system must maintain an awareness of “typical” behaviour so that “atypical” behaviour stands out more obviously. To do this however, requires ongoing development of personal profiles of users of a particular system, which in turn involves monitoring their behaviour online. In cases of both attack and prevention of attacks then, users’ privacy risks are compromised.

A related issue is that of control of data, which may be seen as an aspect of privacy (Moore, 2015, 2003) or additional to privacy concerns (Allen, 1999; Macnish, 2018). In either case, the control of data is a critical factor, as once an attack has been successful control is lost. The data may then be used for a variety of ends, not only relating to violations of privacy but also for political or other gain, as was the case with Cambridge Analytica (Cadwalladr and Graham-Harrison, 2018), where the problem was not only privacy concerns, but also the control of users’ data, which enabled discrete, targeted political advertising concerning the UK’s referendum on membership of the EU and the US presidential election, both in 2016 (Ienca and Vayena, 2018).

While the European Union has sought to resolve concerns with privacy and control of data through the introduction of the General Data Protection Regulation (EU Parliament, 2016), this has raised its own concerns. While European companies must follow strict regulations in developing SIS-related algorithms when it comes to accessing personal data, the same only applies to non-European companies when they practice in Europe. This leads to a concern of

“data dumping, in which research is carried out in countries with lower barriers for use of personal data, rather than jump through bureaucratic hurdles in Europe. The result is that the data of non-European citizens is placed at higher risk than that of Europeans” (Macnish and van der Ham, 2019, p. 8).

Incidental findings also fall under this category, as data derived from regular scans with the goal of profile-building can uncover new information about an individual which they did not want to reveal. Decisions should be made in advance on how to reveal that information and to whom it should be revealed; for example, the discovery that an employee is looking for another job.

2.4 Vulnerabilities and disclosure

An awareness or a duty to find vulnerabilities in a network which leave it open to an attack can help cybersecurity professionals understand the magnitude of a particular attack. However, disclosure of vulnerabilities to a particular authority, such as the company responsible, also risks the leak of that vulnerability from the responsible authority to communities of hackers so that that network or others may be exploited (Macnish and van der Ham, 2019, p. 9). If vulnerabilities are made public

then the public visibility of a system and therefore its commercial viability may be threatened. For example, Wolter Pieters has pointed out the challenge of exposing vulnerabilities in e-voting systems: prior to an election and the systems will not be trusted; after an election and the election result will be called into question. However, if the vulnerability is not disclosed then an attack may occur which genuinely compromises the election. A related issue here is whether cybersecurity researchers looking at the techniques and practices of hackers should have a duty to expose vulnerabilities as an act of professional whistleblowing. By rendering this a duty, there is less pressure on the professional to have to decide what is the right thing to do in a particular case, such as when competing financial interests may argue against such revelations (Davis, 1991)

2.5 Competence of Research Ethics Committees

Within universities and many research institutions, Research Ethics Committees (REC or Institutional Review Boards) oversee applications for research to provide protection for research participants. However, RECs are often composed of experts in ethics who have limited awareness of cybersecurity practice, or computer scientists who lack ethical expertise. An example of this occurred when potentially harmful research was carried out on non-consenting individuals in totalitarian states which effectively tested the firewalls of those states (Burnett and Feamster, 2015). While this research clearly put individuals at risk without their consent, at least two RECs determined that the research was not of relevance for ethical review because it did not concern human participants or personal data. It did, however, concern IP addresses which could easily be linked to a human person, putting that person at risk (Macnish and van der Ham, 2019). Furthermore, it should be noted that these are concerns which arise in institutions with access to a REC. As pointed out by Macnish and van der Ham (2019), many private companies do not have any ethical oversight facilities.

2.6 Security issues

Given the aforementioned definition of security as the absence of threat to acquired values, the maintenance of good security is an ethical issue, as without it commonly-held values may be compromised. “Insufficient funding, poor oversight of systems, late or no installation of “patches” (fixes to security flaws), how and where data are stored, how those data are accessed, and poor training of staff in security awareness” (Macnish, van der Ham, 2018, p.11-12) are therefore all instances of ethical concern.

2.7 Trust and transparency

Trust is an issue which connects the cybersecurity expert to the users who are being protected. Relating back to concerns regarding the risks inherent in publicizing vulnerabilities, there are pressing issues concerning transparency, such as

“how far to push transparency: should it extend to government agencies or even other companies? On one hand sharing information increases vulnerability as one’s defences are known, and one’s experience of attacks shared, but on the other it is arguably only by pooling experience that an effective defence can be mounted” (Macnish and van der Ham, 2019, p. 14).

Pieters argues that trust in a person goes hand-in-hand with the explanation that a person gives (Pieters, 2011). Artificial agents hence need to explain their decisions to the user, such as how

security is maintained in online transactions (Pieters, 2011, p. 53). He argues that there is a need for better understanding of the relationship between explanation and trust in Artificial Intelligence (AI) and information security. Glass et al. concluded that trust depends on both the detail of explanations provided and on the transparency of the system (Glass et al., 2008). From a



From a cybersecurity perspective, what matters is how to communicate *whether* the system is secure, *why* it is secure, or *how* it is secure.

cybersecurity perspective, what matters is how to communicate *whether* the system is secure, *why* it is secure, or *how* it is secure. In SIS, explanations are typically provided by the system itself, while in information security the explanations are provided by the designer (Bederson et al., 2003). Pieters argues that the role of explanations consists, at least in part, in acquiring and maintaining users' trust. He further exposes the concept of "black boxes" which, together with trust and explanation, is a fundamental concept in cybersecurity, where the precise algorithm and associated decision-making techniques may become invisible within SIS systems (Pieters, 2011).

Furthermore, through applying Bruno Latours' actor-network theory (Latour, 2005) Pieters highlights several issues with explanations and trust in information systems. He notes that explanations can be different depending on the actors who are explaining the system or technology. For example, a government seeking to protect the democratic credentials of an election, or a business with a commercial interest in keeping the source code secret, will have different explanations for an e-voting system (Pieters, 2011, p. 57). In the same way, Pieters notes that delegation of technical aspects relating to the SIS will lead to a new actor who will not necessarily have the same abilities to explain the system as the designer.

Pieters also notes that explanations can have different goals, such as transparency versus justification. He argues:

"Explanation-for-trust is explanation of how a system works, by revealing details of its internal operations. Explanation-for-confidence is explanation that makes the user feel comfortable in using the system, by providing information on its external communications. In explanation-for-trust, the black box of the system is opened; in explanation-for-confidence, it is not" (Pieters, 2011, p. 57).

In the field of cybersecurity, as elsewhere in security, explanation of the security capabilities of the system to the user is an important requirement. "This is especially true because security is not instantly visible in using a system, as security of a system is not a functional requirement" (Pieters, 2011, p. 58). For example, it is not possible to infer that if a system gives good results then that system is secure. As Pieters warns, a criminal might have changed the results of voting without anyone noticing. Uncertainty is a feature within these systems and given that security is often added to the system without being integral to it, it is feasible that the system can function without compromise being detected.

2.8 Risk

Consideration of who will decide what risks will be taken, what are the acceptable risks, and how risk is calculated (Hansson, 2013; see also Wolff, 2010) is important in cybersecurity. One of the arguments given for not requesting informed consent in the case described by Burnett and Feamster regarding the non-consensual importing of malware onto user's computers to test firewalls was that, in the opinion of the researchers, there was only a limited risk of harm to the subject (2015, p. 664). However, it does not take much reflection to identify the risk to users who live in states where censorship is an issue, leading to potentially difficult situations (Byers, 2015; Macnish and van der Ham, 2019). Furthermore, it has been demonstrated that different groups of society tend to assess risk differently, with the acceptable risk threshold of white men being significantly higher than that of women or ethnic minorities (Hermansson, 2010, 2005).

2.9 Responsibility

The locus of responsibility for protecting against, and paying for protection against, cyberattacks is an ongoing issue (Guiora, 2017, pp. 89–111). It is not clear whether companies should be left to fend for themselves against hostile state-sponsored attacks, or whether governments should provide at least some financial support for them. Given the aforementioned potential to view cyberattacks as justification for declaring war, it is important to ask the degree to which the state should shoulder “responsibility for protecting its own economy on the internet as it does in physical space, by providing safe places to trade” (Macnish, van der Ham, 2018, p.14).

Cybersecurity is usually taken to concern attacks from outside an entity rather than inside, for example using firewalls against incoming traffic (Cleeff et al., 2009). Yet the development of technology allows for a global environment in which many businesses provide third parties access to their own networks, thus expanding the boundaries of what, or who, may be seen as “inside”. This extends to “mobile devices [that] can access data from anywhere, and smart buildings [which] are being equipped with microchips that constantly communicate with each other” (Cleeff et al., 2009, p. 50). Cleeff et al refer to this as “deperimeterization”, implying that not only is the border of the organization's IT blurred, but also that the accountability for that border is dispersed. For example, “if the organization makes a decision to apply a certain data protection policy in its software, the data may in fact be managed by a different organization. How will the organization that actually manages the data implement and verify this?” (Cleeff et al., 2009, p. 51).

2.10 Business interests and codes of conduct

Competing interests are frequently perceived in security and profit. This may be seen as a zero-sum game in which any money spent on security is money which cannot be spent on increasing profit. However, this is clearly a flawed approach given the financial costs incurred in suffering a successful cyberattack. An example here is the decision of Marissa Meier, then CEO of Yahoo, not to inform the public of attacks in 2013 and 2014 regarding their accounts, most likely because such a revelation could have led to a loss in profit. Yet, when it became known, it devastated the company (Stone, 2017). In response to similar concerns, Macnish and van der Ham argue for the necessity of guidance on disclosure of vulnerabilities:

“public-spirited motivations should be protected from predatory practices by companies seeking to paper over cracks in their own security through legal action. However, current conventions as to how to proceed with disclosure of vulnerabilities seem to be skewed in the favour of corporations and against the interests of the public” (Macnish and van der Ham, 2019, p. 9).

They note that ethical problems cannot be solved easily, but propose creating a code of conduct for cybersecurity to provide guidance and a degree of consensus within the cybersecurity community regarding appropriate action in the face of attacks.

3. The Case Study of a Cybersecurity company using SIS

The literature review demonstrates a variety of ethical issues in cybersecurity. In this section our goal is to present the ethical problems that arise in practice. We aim to compare practice with academic literature concerning ethical issues of SIS in cybersecurity. This will help to inform both sides if there is a lack of understanding of the problems, and to enable mutual learning.

This case study focuses on the ethical challenges that SIS bring in cybersecurity to shed some light on the risks of this sector and how they are currently minimized. The interview was conducted with four employees as a group at Nokia Company Headquarters in Helsinki. All are experts in the Nokia cybersecurity research team: Interviewee 1, a doctoral student; Interviewee 2, a coder who focuses on core network security; Interviewee 3, a coder who focuses on trusted computing; and Interviewee 4, a coder with background in machine learning.

3.1 Description of SIS technologies being used in Nokia

Background research was initially conducted through investigating Nokia’s website and public documents from conferences. This was then supplemented by the interviewees’ explanations of the technical capabilities of the technologies used at Nokia.



Clients’ data gathering capability has expanded faster than their data analysis capability, so that they increasingly gather data that has no obvious purpose.

Nokia is a global digital communications company. It is involved in cloud computing, artificial intelligence, machine learning, internet of things and the infrastructure of mobile networks, including 5G. Nokia’s website refers to a combination of analytics and augmented intelligence (Nokia, 2018a), but the company also specialize in research and development (R&D) through Bell Labs, where it conducts research for “the next phase of human existence” (Nokia, 2018b). Among its research, one can find the “virtual sixth sense”, which Forbes magazine described as a “look at where exponential trends in technology development, personal and device connectivity and data collection and analysis might take business, the global economy and society at large”

(Marko, 2015). Markus Weldon, president of Bells Lab, in his book *The Future X Network*, shows the development of technology and the relation with global economy and society, by acknowledging the “scale of changes wrought by a nexus of global, high-speed connectivity, billions of connected

devices (IoT), cloud services and non-stop data streaming, collection and big data analytics” (Marko 2015).

These technologies are “changing our world” and Nokia sees itself as “driving innovation and the future of technology to power this digital age and transform how people live, work and communicate” (Nokia, 2018c). These technologies use data, including personal data from customers and metadata from phone networks. During the interview, Interviewee 1 argued that they do not use AI, but they do use statistics and analytics, such as products that use machine learning (ML) and data collection to identify malware. They also use analytics to create rules for developing effective firewalls for the network. However, Interviewee 3 noted that AI is still part of the research and the internal projects:

“we do not sell a brain... or the giant quantum computing brain that solves all the problems, but for a very long time, planning has been used in many products, you can consider some configuration algorithms that can be considered as AI, these things exist, but not in the futuristic sense” (Interviewee 3 2018)

The term “cybersecurity” appears in different articles across the Nokia website. The cybersecurity research team at Nokia developed a report on security for 5G networks which has served as guidance for the European Union. They analyse bulk datasets to help clients (communications providers rather than end users) maximize efficiency and thus profit, while at the same time providing security such as malware detection to protect the end user from attacks.

SIS applications vary due to the amount and variety of data that Nokia gathers from its customers, as well as the diverse needs of those customers. Many of these needs could not be met without SIS technology, as they would be impossible to perform by hand. For the most part, Nokia cybersecurity research team use rule-based applications for sorting information which is then evaluated by a person. Interestingly from an ethical point of view, Interviewee 1 pointed out that clients’ data gathering capability has expanded faster than their data analysis capability, so that they increasingly gather data that has no obvious purpose.

Table 1

Description	Organisation 1
Organisation	Nokia
City	Helsinki
Sector	Cybersecurity/Telecommunications
Name	Interviewee 1
	Interviewee 3
	Interviewee 2
	Interviewee 4

Length	136 minutes
--------	-------------

3.2 The effectiveness of using SIS by Nokia

As noted above, the use of AI and ML is due to the complexity and amount of data retrieved from clients' systems. According to Nokia's website, cloud computing, AI, ML, IoT and 5G Networks are changing the world and they have the power to "transform how we live, work, and communicate" (Nokia, 2018c). Much of this is due to the fact that the operations now performed would previously have been impossible owing to the sheer volume and complexity of the data.

Nokia has been using SIS in cybersecurity for some time. SIS allows the team to discover attempted hacks or other misuse such as fraud or the use of fake base stations (imitating a legitimate mobile phone tower in order to collect personal data). Current technology allows pre-filtering and sorting, but is less effective at identifying or responding to targeted attacks which are more sophisticated than bulk attacks. Interviewee 4 described a detection system they had worked on:

"one of their security teams was working on malware detection for telecom software for operators, and that research went into Netguard. That software ended up in systems that will protect end-users from malware that could be installed into phones. This is more at the operator level, not like an antivirus which is for a phone users-level" (Interviewee 4 2018)

4. Ethical Implications in Cybersecurity

In this section we will look in greater depth at the ethical issues discussed during the interview conducted with the four employees at Nokia. The issues which were uncovered in the interview widely reflect those found within the literature. It is however important to note that SIS use is growing rapidly: the technology is evolving and huge amounts of data are being collected. Generally, the interviewees explained that there is a lack of joint efforts from the ethical review boards within the company and there is a need to continue and improve the dialogue between the ethical and technical fields.

The ethical issues discussed in the interview comprised of privacy; internationalisation, standardisation and legal aspects; monetisation issues; anomalies; policy issues, awareness and knowledge; security; risk assessment; and mechanisms to address ethical issues. Each of these will be discussed in greater depth in this section.

4.1 Privacy

Nokia takes privacy seriously. Interviewee 2 pointed out that they were involved in drafting the document for 5G networks concerning privacy and the future of 5G security, which became a guideline for the European Parliament and for national legislatures. Privacy was seen during the interview as one of the most important underlying ethical issues. Concerns about users' and companies' privacy were evident. Some discussion was held around the issue of "quantifying privacy" (how does one measure privacy?). However, further problems arise in sharing data with

customers, which to Nokia are telecommunications providers rather than end users, as the team often do not know what the customer knows. Hence, data that may be anonymous in one dataset may be re-identified when cross-referenced with another dataset which is proprietary to the customer.

“Sometimes if you manage to monetise your data, whatever data we’re talking about, not just telco, and a buyer also has access to other sources of data that cross-correlate with your data, or have similar identifiers, you can never predict this as a seller of data. The end result is that your customer basically gets access to something that he can just map back to the original data, pretty much, by just looking at two fields and just cross-correlating. And you can never predict this. In that sense it’s already doomed from that point of view, but it’s a best effort sort of thing, and within a narrow context it still works” (Interviewee 4 2018)

Differential privacy, a technical “fix” for privacy concerns employed by Apple, among others (Apple, 2018) was also discussed. The team noted that differential privacy does not work with complete reliability because you can never be sure of what the data can lead to. Hence uncertainty also becomes an important issue in relation to privacy. Furthermore, Interviewee 3 considered that we should have a numerical measurement for privacy but that, they suggested, would not be possible.

4.2 Internationalization, standardization and legal aspects

Given the global nature of telecommunications, international cloud computing and the IoT, there is an increasing need for global regulation. Interviewee 4 introduced the problem of an application on mobile phones that sends data to China every 5 minutes: in such cases, which state’s laws should be followed, those of the country where the user currently is, those of the state in which the user is registered as a citizen, those of the country where the operator is located, or those of the country of origin of the application operator, in this case China. Interviewee 2 argued that one of the issues that they have encountered is that the customer data comes from everywhere in the world. As Nokia is a global company, it works also in places such as the Middle East or Asia, and not only receives information from European customers but from other parts of the world. She raised the question as to whether it would be ethical to see data from everywhere in the world when there are no clear guidelines. Interviewee 3 also pointed out the issues with different regulations:

“Northern Europe is doing well; Germany is most strict. Italy, Spain, Portugal strict. [Some others do not] really care” (Interviewee 3 2018)

Interviewee 2 explained that European laws are much stricter than most other nations, and in following the European laws Nokia restricts data sharing. It hence does not share data with third parties, and has just one person looking at data unless there is a clear need for more. Interviewee 4 also pointed out that there is a Nokia “sensitive data handling policy”, which involves rules for data encryption and storage, which is closely monitored. Furthermore, special clearances are required to access some data, although the cybersecurity research team is in a “privileged” position to receive such data. Interviewee 4 noted that some data is not allowed to be copied, just processed on the server.



There was ... general agreement that what mattered was not just being compliant with the letter of the law, but also the spirit.

Interviewee 3 added that governments are also involved and there is a need for standardised practices:

“In telco we have some interesting issues that are coming up. It’s not just telco versus attacker. You have two other players. Standardisation, where you try and make a level playing field for everyone. Then you’ve got governments, [say] security services, who might say, “Well, let’s get rid of encryption, because bad guys use encryption” (Interviewee 3 2018).

Interviewee 3 explained that the spirit of GDPR is not about compliance but about risk management, and companies have to show that they are doing due diligence and minimizing the risks as much as possible. As an example of this, Interviewee 2 suggested that in order to review data, you can ask for one group of phones instead of having access to the whole network, which would compromise a large number of people. In contrast, Interviewee 3 argues that according to US laws, the National Security Agency (NSA) are allowed to collect data of domestic individuals which they then send to the UK for analysis. There was also general agreement that what mattered was not just being compliant with the letter of the law, but also the spirit. The team noted that Finnish regulators in particular are not only concerned with compliance but also the motivations behind activities, and where the boundaries lie as to the limits of acceptable practice, which speaks of a high ethical standard.

4.3 Monetization issues

The team felt that the existence of public clouds and data sharing with different companies such as Amazon increases the potential for monetization of data. Different stakeholders are looking to monetize data, which is very privacy sensitive. Interviewee 1 argued that these new advances and technologies are helping to monetize customer’s data, like targeted advertisements. Interviewee 4 added that some companies are seeking to monetize data within the current regulations, which is something that, according to Interviewee 4, must be questioned:

“are we doing the best we can before we monetize it, selling it, whether using it for mining – Is anonymization and privacy worth it? Can we prove to a certain knowledge, mathematically, that this is anonymized... can we quantify that point?” (Interviewee 4 2018)



Some operators and senior managers ... are guilty of “off-loading perfect expectations to machines” (Interviewee 1 2018).

However, the team agreed that not all operators have cybersecurity people, and not many people are working on telecommunications cybersecurity within operators. Thus, people that have expert knowledge are rare in this field. As Interviewee 2 pointed out, there are relatively few European security teams; companies such as KPN and Orange have one, but not every operator does.

Furthermore, and related to the lack of security expertise, the team felt that there is a need to manage customers’ expectations. Many customers place a high value on SIS even though they do not understand it or the level of security it can engender. Some customers “want perfect security right from the start” (Interviewee 3 2018). In addition, these expectations also hold true among some operators and senior managers who are

guilty of “off-loading perfect expectations to machines” (Interviewee 1 2018).

4.4 Anomalies

Interviewee 4 pointed out that in cybersecurity there is a need to search actively for anomalies. These have arisen for the team in the case of identifying fake base stations. Interestingly, Interviewee 4 mentioned that the U.S. has been trying to stop the news about these fake base stations because knowledge of their existence may damage the trust that people put in the networks.

“in China you have fake antennas or fake base stations which can push advertisements etc. to people’s phones, and there have been thousands in China... In France, these fake base stations are used by the police to catch all the phones, not to do something malicious because is kind of the police enforcement, these are the so-called anomalies, when you have for a short period of time a phone for which service is delayed” (Interviewee 4 2018)

Interviewee 2 explained that they did not encounter many fake stations, but rather, they see attacks which seem to come from other network operators. e.g. a telecommunications provider in Barbados asking another telecommunications provider in Finland for the location of a Finnish subscriber, when there is no obvious technical need (such as to enable roaming). In such cases there is clearly no reason to give that information. Nokia also makes use of firewalls to prevent attacks, but these need to be tailored to avoid false positives and blocking too much legitimate traffic.

4.5 Policy issues, awareness and knowledge

Nokia holds mandatory ethics training for all staff, which covers privacy compliance. However, Interviewee 3 suggested that it could be far more effective than is currently the case:

“it appeals to the lowest common denominator for everyone, when it says things like – you should apply privacy by design, you should use methods and processes...” (Interviewee 3 2018)

However, Interviewee 2 offers a more positive perspective, arguing that it is making both companies and users aware of the problem:

“at least the message gets through to every employee, that somehow we care, that you should think about that” (Interviewee 2 2018)

Interviewee 3 noted that customer data is strictly regulated at Nokia, with codes of conduct and legal frameworks to guide behaviour. The company’s legal framework also provides a base from which to determine ethical decisions. Interviewee 4 explained that they had a data-security course which was mandatory, and so there are serious attempts to deal with the ethical implications of the work.

Moreover, Interviewee 3 argued that users should also have technical knowledge and the technical competence regarding practicing safe behaviour online.

The team agreed that there is a need for more regulation.

Interviewee 3 argued that privacy and data analytics should become regulated industries, similar to car management software, or software for medical devices, in which industries you have to keep the source code for 50 years, and it has to be documented and signed before it can be used. Interviewee 3 also mentioned that it is worth paying attention to the level of training for engineers

regarding the need for an ethical background. Interviewee 3 explained that every engineer has to make ethical decisions at some point. As such it is important that engineers are free to object and refuse to participate in certain projects. Interviewee 2 added that they have an Ethics section in Nokia that helps with these issues, providing support to employees who may have concerns. Furthermore, they stated that there is no code of conduct for cybersecurity.



Compliance training could be improved, but it gets the message agree that privacy is important.

4.6 Security

Interviewee 3 described how IT departments in some companies send internal “phishing mails” (emails attempting to trick the recipient into giving private information) to test their security, and the problem is that employees tend to have a high record on clicking on them, demonstrating a weak level of security awareness. Interviewee 3 also explained that Nokia, amongst other companies, have a “hackathon” every year to discover security flaws. Interviewee 4 mentioned that they have companywide encryption policies for some sensitive materials, which is easy to use now, but that was not the case in the past. Interviewee 4 felt that security is of importance at Nokia, but, as Interviewee 1 pointed out, most research is conducted internally so that there is a lack of publications, at least for the public space. This leaves a number of unanswered questions, such as:

“who is attacking your system and what are they after - this hasn't been researched properly, or has been researched but not publicly available” (Interviewee 3 2018)

4.7 Risk Assessment

Interviewee 4 noted that there is a lack of risk assessment regarding some key aspects of security, such as the risk of not having security protocols, or the comparative risk of predictive versus reactive strategies. Interviewee 3 said that they had a PhD student currently studying cybersecurity attacks, and one of the things that came out of this research is that the attackers do not necessarily go for the weakest part of the system, because that is not where “the big game are”. Therefore, this shows the need to have cybersecurity teams that will look for security pitfalls in every part of the system, even in the parts that are considered more secure by design.

Interviewee 3 further stated that there is a problem in that the technology they work with can be misused, e.g. used for spying on different countries. Interviewee 2 continued that even if the government has access to this information, the question still remains as to the extent to which citizens can be sure that no one else has the same access. What if a government's position changes, such as that of Germany in the 1920s and '30s? There is very little that can be done under such circumstances.

4.8 Mechanisms to address ethical issues

During the interview it was noted that there is a need for a culture of openness and challenge in organisations, and that the current paradigm of ethical standards in the use of SIS in cybersecurity is present but not developed. While the GDPR has improved general levels of awareness of cybersecurity and the importance of privacy, there is a need for ethical training for current engineers, as well as to develop stricter codes of conduct for this sector. The external regulations of, for example, targeted advertising and the issues of internationalization require consideration. Furthermore, while GDPR has a strong impact on privacy in Europe, other countries allow companies to gather data more freely.

Nokia has a number of security strategies which go some way to addressing ethical concerns. Mandatory training sessions are held annually and policy documents provide guidance. These are supplemented by a culture of challenge and openness in which employees feel free to share their concerns and step back from working on a project with which they have ethical concerns. There are also security measures put in place to keep sensitive data secure, such as limiting the machines on which the data can sit, and operating a security clearance system such that only certain people are cleared to access the data.

Engagement with different stakeholders, such as the internal Nokia units, the academic community, regulators and government agencies, clients and end users was deemed both desirable and beneficial for all.

5. Conclusion

Table 2

Issues arising in Literature Review	Issues arising in Interview
Similarities	
Protection from harm	Protection from harm
Privacy and control of data	Privacy and control of data
Competence of research ethics committees	Competence of research ethics committees
Security issues	Security issues
Risk	Risk Assessment
Business interests	Monetization issues
Codes of conduct	Policy issues (awareness and knowledge) and mechanisms to address ethical issues
Responsibility	Internationalization, standardization and legal aspects
Differences	
Vulnerabilities and disclosure	Anomalies

Trust and transparency	
Informed consent	

The literature review and the interview highlight a correlation between academic understanding of the ethical issues in cybersecurity and those working for the cybersecurity industry. However, both have also shown a lack of joint efforts from academia and engineering, and the need to improve the dialogue between the two. There is concern that the level of technical abstraction of university-based development stifles ethical oversight of the development of new SIS technologies in computer science. At the same time, there is a need to include ethical oversight in industry, with clearer codes of conduct for the cybersecurity community. One of the strongest arguments from the team at Nokia was the lack of clear codes for international practice. As SIS technology is being developed with cloud computing, and the facility to acquire data from all over the world grows, so there is a need to improve ethical protocols for companies.

Overall, it was shown that ethical concerns regarding SIS in cybersecurity go further than mere privacy issues. As it is a sector that will grow in the coming years, incorporating ML and the IoT, the importance of cybersecurity, and thereby the ethics of cybersecurity, will become more important.

Among the ethical issues we found the following: informed consent, protection from harm, disclosure of vulnerabilities, biases, the nature of hacking, trust, transparency, the necessity for a risk assessment in cybersecurity, responsibility between companies, government and users. Interestingly, the issue of monetization (how far can one ethically go to monetize customer's data) appeared in the interview but is not one that has been widely discussed in the academic literature.



One of the strongest arguments from the team at Nokia was the lack of clear codes for international practice

5.1 Implications of this report

This report exposes some of the weakest part of SIS technology and the importance of cybersecurity, by supporting the claim that there is a need to improve the ethics of research in SIS. The cyber world is forming an important part of society and in some areas at least, albeit not among the interviewees for this case study, there is a lack of understanding of the ethical problems that come with this, which can bring damage to many stakeholders.

5.2 Future research

This report argues for the need for multi-disciplinary studies between academia and the technical community to prevent ethical concerns from being undervalued. Future research goes hand in hand with legal implications, particularly at the international level, as well the need to create clearer codes of conduct for businesses and international practices, and the necessity to increase the cybersecurity teams within companies.

6. References

- Allen, A.L., 1999. Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm. *Conn. L. Rev.* 32, 861.
- Apple, 2018. Privacy - Approach to Privacy [WWW Document]. Apple (Latin America). URL <https://www.apple.com/lae/privacy/approach-to-privacy/> (accessed 12.17.18).
- Bainbridge, L., 1983. Ironies of Automation. *Automatica* 19, 775–779. [https://doi.org/10.1016/0005-1098\(83\)90046-8](https://doi.org/10.1016/0005-1098(83)90046-8)
- Baldwin, D.A., 1997. The concept of security. *Review of international studies* 23, 5–26.
- Beauchamp, T.L., 2009. Autonomy and Consent, in: Miller, F., Wertheimer, A. (Eds.), *The Ethics of Consent: Theory and Practice*. OUP USA, Oxford ; New York, pp. 55–78.
- Bederson, B.B., Lee, B., Sherman, R.M., Herrnson, P.S., Niemi, R.G., 2003. Electronic Voting System Usability Issues, in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '03*. ACM, New York, NY, USA, pp. 145–152. <https://doi.org/10.1145/642611.642638>
- Burnett, S., Feamster, N., 2015. Encore: Lightweight Measurement of Web Censorship with Cross-Origin Requests, in: *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, SIGCOMM '15*. ACM, New York, NY, USA, pp. 653–667. <https://doi.org/10.1145/2785956.2787485>
- Byers, J.W., 2015. Encore: Lightweight Measurement of Web Censorship with Cross-Origin Requests—Public Review. Technical Report [http://conferences.sigcomm.org/sigcomm/2015/pdf/reviews](http://conferences.sigcomm.org/sigcomm/2015/pdf/reviews....)
- Cadwalladr, C., Graham-Harrison, E., 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian* Interviewee 3.
- Cleeff, A. van, Pieters, W., Wieringa, R.J., 2009. Security Implications of Virtualization: A Literature Study, in: *2009 International Conference on Computational Science and Engineering*. Presented at the 2009 International Conference on Computational Science and Engineering, pp. 353–358. <https://doi.org/10.1109/CSE.2009.267>
- Craigien, D., Diakun-Thibault, N., Purse, R., 2014. Defining Cybersecurity. *Technology Innovation Management Review* 4, 13–21.
- Davis, M., 1991. Thinking like an engineer: The place of a code of ethics in the practice of a profession. *Philosophy & Public Affairs* 150–167.
- EU Parliament, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L.
- Glass, A., McGuinness, D.L., Wolverton, M., 2008. Toward establishing trust in adaptive agents, in: *Proceedings of the 13th International Conference on Intelligent User Interfaces*. ACM, pp. 227–236.
- Goddard, K., Roudsari, A., Wyatt, J.C., 2012. Automation bias: a systematic review of frequency, effect mediators, and mitigators. *J Am Med Inform Assoc* 19, 121–127. <https://doi.org/10.1136/amiajnl-2011-000089>
- Guiora, A.N., 2017. *Cybersecurity: Geopolitics, Law, and Policy*, 1 edition. ed. Routledge, Boca Raton, FL.
- Hansson, S.O., 2013. *The Ethics of Risk: Ethical Analysis in an Uncertain World*. Palgrave Macmillan.
- Hermansson, H., 2010. Towards a fair procedure for risk management. *Journal of Risk Research* 13, 501–515. <https://doi.org/10.1080/13669870903305903>
- Hermansson, H., 2005. Consistent risk management: Three models outlined. *Journal of Risk Research* 8, 557–568. <https://doi.org/10.1080/13669870500085189>
- Hess, C., Ostrom, E., 2007. *Understanding knowledge as a commons*. The mit press.

- lenca, M., Vayena, E., 2018. Cambridge Analytica and Online Manipulation [WWW Document]. Scientific American Blog Network. URL <https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/> (accessed 7.10.18).
- Johnson, M.L., Bellovin, S.M., Kromyitis, A.D., 2012. Computer Security Research with Human Subjects: Risks, Benefits and Informed Consent, in: Danezis, G., Dietrich, S., Sako, K. (Eds.), *Financial Cryptography and Data Security*. Springer, Berlin, pp. 131–37.
- Latour, B., 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory*. OUP Oxford, Oxford.
- Lundgren, B., Möller, N., 2017. Defining Information Security. *Sci Eng Ethics*. <https://doi.org/10.1007/s11948-017-9992-1>
- Macnish, K., 2018. Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. *Journal of Applied Philosophy* 35, 417–432. <https://doi.org/10.1111/japp.12219>
- Macnish, K., 2012. Unblinking eyes: the ethics of automating surveillance. *Ethics and Information Technology* 14, 151–167. <https://doi.org/10.1007/s10676-012-9291-0>
- Macnish, K., van der Ham, J., 2019. Ethics and Cybersecurity Research. *Journal of Science and Engineering Ethics*.
- ManjilInterviewee 3, M., 2017. *Cybersecurity Ethics*, 1 edition. ed. Routledge, London ; New York.
- Manson, N., O'Neill, O., 2007. *Rethinking Informed Consent in Bioethics*. Cambridge.
- Marko, K., 2015. The Omni-Connected World: Bell Labs Plans For Future Of Connected Everything [WWW Document]. Forbes. URL <https://www.forbes.com/sites/kurtmarko/2015/10/27/omni-connected-world/> (accessed 12.17.18).
- Miller, F., Wertheimer, A. (Eds.), 2009. *The Ethics of Consent: Theory and Practice*, 1 edition. ed. OUP USA, Oxford ; New York.
- Moore, 2015. *Privacy, Security and Accountability: Ethics, Law and Policy*. Rowman & Littlefield, London ; New York.
- Moore, A., 2003. Privacy: Its Meaning and Value. *American Philosophical Quarterly* 40, 215–227.
- Nichols, S., 2016. St Jude sues short-selling MedSec over pacemaker “hack” report [WWW Document]. The Register. URL https://www.theregister.co.uk/2016/09/07/st_jude_sues_over_hacking_claim/ (accessed 7.4.18).
- Nokia, 2018a. Software - Home [WWW Document]. Nokia Networks. URL <https://networks.nokia.com/software> (accessed 12.17.18).
- Nokia, 2018b. Nokia Bell Labs [WWW Document]. Nokia. URL <https://www.nokia.com/innovation/nokia-bell-labs/> (accessed 12.17.18).
- Nokia, 2018c. Our vision [WWW Document]. Nokia. URL <https://www.nokia.com/about-us/who-we-are/our-vision/> (accessed 12.17.18).
- Pieters, W., 2011. Explanation and trust: what to tell the user in security and AI? *Ethics Inf Technol* 13, 53–64. <https://doi.org/10.1007/s10676-010-9253-3>
- Singer, P.W., Friedman, A., 2014. *Cybersecurity: What Everyone Needs to Know*. OUP USA.
- Smith, P.T., 2018. Cyberattacks as Casus Belli: A Sovereignty-Based Account. *Journal of Applied Philosophy* 35, 222–241. <https://doi.org/10.1111/japp.12169>
- Sobers, R., 2018. 60 Must-Know Cybersecurity Statistics for 2018 [WWW Document]. Varonis Blog. URL <https://www.varonis.com/blog/cybersecurity-statistics/> (accessed 12.17.18).
- Spring, T., 2016. Researchers: MedSec, Muddy Waters Set Bad Precedent With St. Jude Medical Short. The first stop for security news | Threatpost.
- Stone, N., 2017. The Yahoo Cyber Attack & What should you learn from it? [WWW Document]. Cashfloat. URL <https://www.cashfloat.co.uk/blog/technology-innovation/yahoo-cyber-attack/> (accessed 12.17.18).

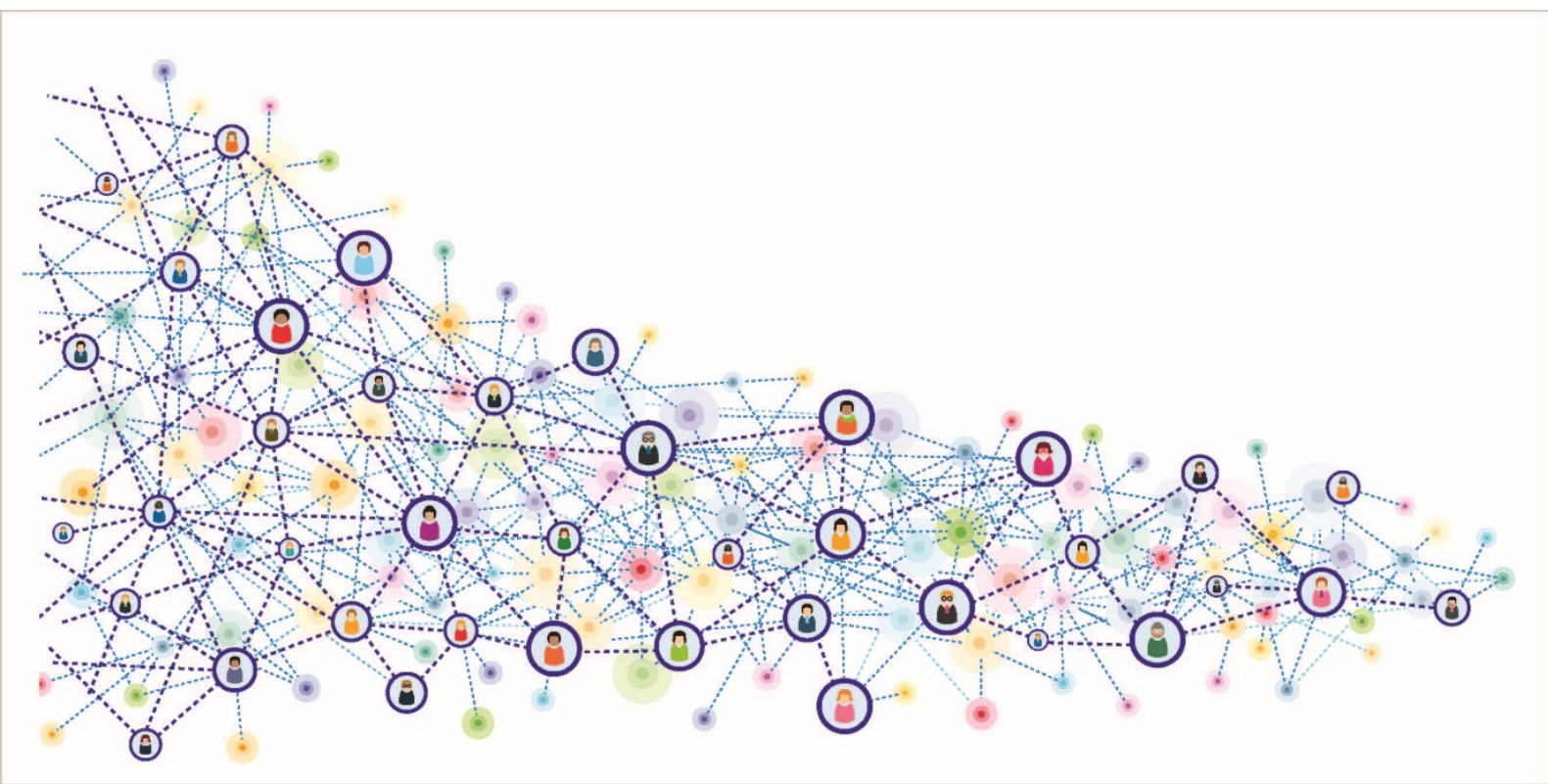
- Tucker, E., 2018. Cyber security – why you’re doing it all wrong [WWW Document]. ComputerWeekly.com. URL <https://www.computerweekly.com/opinion/Cyber-security-why-youre-doing-it-all-wrong> (accessed 12.17.18).
- Wolfers, A., 1952. “National Security” as an Ambiguous Symbol. *Political Science Quarterly* 67, 481–502. <https://doi.org/10.2307/2145138>
- Wolff, J., 2010. Five Types of Risky Situation. *Law, Innovation and Technology* 2, 151–163. <https://doi.org/10.5235/175799610794046177>

CS09 – Retail and Wholesale Trade



SHERPA

Case Study - Customer Relation Management, Smart Information Systems and Ethics



This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641



Document Control

Deliverable	Deliverable 1.1.: Case Studies
WP/Task Related	WP 1: Representation and Visualisation
Delivery Date	31 January 2019
Dissemination Level	Public
Lead Partner	University of Twente
Contributors	Kevin Macnish, UT; Ana Fernandez, UT
Reviewers	Mark Ryan, UT
Abstract	This report provides an overview of the current implementation of SIS in the customer relations management (CRM). It also identifies the positive and negative aspects of using SIS in CRM, including ethical issues which could arise while using SIS in this area. One company working in the industry of telecommunications (Elisa) is analysed in this report. Further specific ethical issues that arise when using SIS technologies in Elisa are critically evaluated. Finally, conclusions are drawn on the case study and areas for improvement are suggested.
Key Words	Customer relations management, smart information systems, big data, ethics

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes
0.1	14/11/2018	Ana Fernandez		
0.2	21/11/2018	Kevin Macnish		Revision
0.3	24/11/2018	Mark Ryan		Revision
0.4	4/12/2018	Kevin Macnish		Revision
1.0	22/1/2019	Kevin Macnish		Revision

Contents

Executive Summary	249
Customer Relationship Management and SIS: An Ethical Analysis	250
1. The Use of SIS Technology in Customer Relationship Management	251
2. Ethical Issues of Using SIS in CRM	253
2.1. Autonomy, Control and Manipulation	254
2.2. Privacy and Knowledge	254
2.3. Informed Consent	255
2.4. Bias	256
2.5. Responsibility and Trust	256
3. Case Study: a Telecommunications Company using CRM SIS	257
3.1. Description of SIS technologies being used in Elisa	257
3.2. The Effectiveness of Using SIS for Elisa	259
4. Ethical Analysis of CRM Using SIS	259
4.1. Intrusion and Regulatory Differences	260
4.2. Privacy and Security	260
4.3. Bias and Manipulation of Data	261
4.4. Responsibility and consent	261
4.5. Transparency and the company's vulnerability	262
5. Conclusion	262
5.1. Limitations	264
5.2. Contribution to Knowledge	265
5.3. Implications of this Report	265
5.4. Further Research	265
6. References	266

Executive Summary

Smart information systems (SIS - Big Data and artificial intelligence) are used in Customer Relations Management (CRM) to help manage large customer databases and improve customer interaction by companies. This case study involves research into the Finnish telecommunications provider Elisa regarding their use of SIS in developing CRM. This they use primarily for assessing “churn”, the drop-off rate of customers choosing not to re-subscribe to Elisa services, and for improving customer service by monitoring customer activity on Elisa’s website. SIS has the potential to improve both of these areas through developing an understanding based on patterns of behaviour.

A literature review of ethical issues facing the use of SIS in CRM reveals that there are a number of such issues. These include autonomy, control and manipulation of people, privacy, customer knowledge as to what happens with data pertaining to them, algorithmic bias, responsibility of companies, governments and individuals, trust and informed consent. The interview held at Elisa demonstrated that many of these issues are recognised and encountered by practitioners operating in SIS. Informed consent and trust were not discussed in the interview while global approaches to ethics was raised in the interview in a manner not seen in the literature review.

Overall, this case study evaluates how ethical issues found within the SIS literature correlate with those identified, and tackled, in the business practice of CRM.

Customer Relationship Management and SIS: An Ethical Analysis

Customer relationship management (CRM) deals with the processes and systems that support business strategies to build long-term and profitable relations with customers (Ngai et al. 2009). The rapid development of the digital world has changed marketing models by transforming CRM practices and relationships between customers and companies. Easier access to customers' online data (through social networks, search engine history, or through the creation of cookies and other tracking systems) allow companies to gather a huge variety of information about customers. Such access also allows companies to create cloud systems which gather and compile the data, and strategize and automate CRM practices.

Advances in Artificial Intelligence (AI) and Machine Learning (ML) have also had a significant role in business development since the turn of the 21st century, with many of these developments being incorporated into new CRM practices. Braun and Garriga (2018) argue that the ML approach to Big Data and CRM overcomes mere statistics or the classification of data and goes one step further towards systems which employ machine learning. This, they claim, results in an optimization and automation of processes in the process of purchasing goods and services. They state that,

“with advanced data engineering, we blend data from all collected data sources...and build ML models that will accurately predict the propensity of a customer to churn [cease to be a customer of the company] based on the stored digital traces... Our models predict the propensity to buy a new product” (Braun A., Garriga G. 2018, p. 667-68).

Thus, Big Data is having a significant impact on the ways in which customers are attracted to, and retained by, an organisation. It is therefore important to study the influence on and ethical implications of these developments for customers.

This case study focuses on determining which ethical issues arise in the use of Smart Information Systems (SIS) in CRM and how can they best be addressed. This will be carried out by the study of the key issues within a literature review and by an interview with an employee working at the Finnish Telecommunications Company Elisa⁵³. Elisa currently uses CRM to maintain a strong customer base by engaging with customers throughout their contract, and especially when the contract is due to expire. At this key time for the company, customers may choose a contract with a different company (“churn”). CRM is also helpful in engaging with ongoing customer needs, such as maintenance and trouble-shooting.

The aim of the case study is to identify what ethical issues arise from the use of SIS in CRM, whether companies that use SIS for CRM have policies and procedures in place for addressing these concerns, and if practitioners are facing additional issues not addressed in the current literature. The case study is divided into four main sections. Sections 1 and 2 focus on the literature review. Section one reviews the technical aspects of CRM, while section two presents a literature review on ethical issues within CRM. Section 3 focuses on the interview with the employee of Elisa. Finally, section 4 critically evaluates ethical issues that have arisen in the use of SIS technologies in Elisa's use of CRM.

⁵³ Elisa's company website can be found at: <https://corporate.elisa.com> - For more information, go to www.elisa.com - Facebook (@elisasuomi) and Twitter (@ElisaOyj).

1. The Use of SIS Technology in Customer Relationship Management

This section details SIS technology and companies which are developing CRM practices to elucidate how this technology is used in practice. A literature review is conducted on the different ways that CRM is used and implemented.

Hailwood and Gottlieb present a background overview of CRM, and explain that the goals of CRM are “acquiring, developing and retaining satisfied, loyal customers” (Hailwood, J., & Gottlieb, D, 2003). They argue that it is desirable for the overall profit and development of a company to increase the number of profitable customers. It is thus expected that companies which implement CRM successfully will obtain the loyalty of customers. Chen and Popovich (2003) argue that a large part of contemporary CRM requires the implementation of technology. In a similar vein, Winer has charted how the technological revolution has changed the relationships companies have with clients. The most significant aspect of this is increased interaction and improved, customized experience for the customer, such that companies now have a better ability to “establish, nurture, and sustain long-term customer relationships than ever before” (Winer 2001, p.89; see also Blázquez, 2014; Parise et al., 2016; Soudagar et al., 2012). He continues by stating the profitable figures of this new practice:



The goals of CRM are “acquiring, developing and retaining satisfied, loyal customers” (Hailwood, J., & Gottlieb, D, 2003).

“Companies such as Siebel, E.piphany, Oracle, Broadvision, Net Perceptions, Kana, and others have developed CRM products that do everything from track customer behavior on the Web to predicting their future moves to sending direct e-mail communications. This has created a worldwide market for CRM products and services of \$34 billion in 1999, a market that is forecasted by IDC to grow to \$125 billion by 2004” (ibid)

Winer argues that the creation of a customer database is a necessary first step towards establishing effective customer-relationship management (Winer 2001, p.91). Thus, a feature of contemporary market practice has been that companies have acquired large datasets regarding stock and customers, enabling more effective practices of mass marketing.

There are therefore a number of different strategies in CRM in which the analysis of data is being used. Ngai et al. (2009) identify four major CRM dimensions (ibid. p 2593):

Customer identification	is the targeting of users who are most likely to become customers.
Customer attraction	involves direct marketing such as sending emails or coupons.
Customer retention	incorporates understanding user satisfaction, including practices such as customer profiling and one-to-one marketing.
Customer development	includes historical analysis of data with the purpose of predicting future customer desires and behaviours (ibid. 2595).

With the increasing technical and financial ability to manipulate and interpret large datasets, these CRM strategies have employed data analytics, in which the analysis of customer data and behaviours allows the discovery of new and valuable information from customers (ibid). Braun and Garriga (2018) affirm this and note that the development of CRM is reflected in questions about consumers which are based on hypotheses derived from data analysis, such as:

- *“Consumer profile*—by which category can a distinct consumer be described?
- *Interest*—what is the specific consumer interest?
- *Next best product*—what is she most likely to buy next?
- *Cross- and upsell*—what other product or services can be offered?” (Braun A., Garriga G. 2018, p.665).

CRM has therefore become an online behavioural targeting (OBT) practice which comprises the monitoring and tracking of customers’ online behaviour as well as the use of collected data to individually target and understand specific customer segments (Boerman, Kruikemeier, & Zuiderveen Borgesius, 2017).

This has been particularly significant in areas where customer data was collected prior to developments in computing ability. Banks and telecommunications companies, for example, have standardly gathered large amounts of customer information since their inception. Writing in 2001, Winer offered several examples of different companies’ database practices that were already well established at the beginning of the 21st century.

3Com	had created a global database from their global operations storing records of e-mails, contacts, and locations.
Taylor Made	a golfing equipment company, gathered more than 1.5 million golfers’ names, together with addresses and even vacations and birthdays.
Borders	the bookseller, prior to its collapse in 2011, collected all of its customer information into a single database and sent emails tailored to each customer’s reading interests.
Thomas Holidays	a British tour operator, gathered information about individual expenses from customers which enabled them to discover which customers were more profitable (Winner 2001, p.92-97).

In recent years, these practices have become more controversial with the rise of new and easily available analytical tools such as Google Analytics, which, according to Dubois (2015) are used

by 50% of companies. These tools have allowed for different forms of behavioural targeting such as tracking web browsing through the use of cookies and the development of automated monitoring tools. Furthermore, different analyses are standardly made about overall demographics and populations, including geographic locations. For example, the recently-defunct Cambridge Analytica writes on its website that it targets audience groups through collecting more than 5,000 data points for each individual, and over 230 million individual American consumers (Cambridge Analytica, 2017; see also Cadwalladr and Graham-Harrison, 2018).

In contemporary practice, CRM has become based on the technological ability to obtain and analyze customer information. However, with the possibility of tracking and creating profiles of customers, and the increasing ability to gather large swathes of information, concerns have been raised as to the potential for a negative impact. Privacy issues, a lack of control and a fear of manipulation can come with these new and rapidly evolving methods. The next section will focus on these ethical aspects of SIS in CRM.

2. Ethical Issues of Using SIS in CRM

Data analytics is a growing business that has changed the traditional market to a digital one involving the storage and analysis of large quantities of data to offer predictions based on users' behaviour (Braun 2016). Developments in SIS technology pose new challenges and questions on the continuous collection and analysis of data and the impact this can have on consumers. SIS can be seen as a powerful tool that gives new insights and addresses issues such as terrorism or health and disease (Moorthy et al. 2015, p. 75), as well as providing more personalised service (Macnish 2018, p114-17). However, Big Data also risks decreasing user privacy and increasing the potential for companies to control and manipulate customers.

The possibilities for CRM that come with Big Data analysis raise important issues such as:

- ownership of data,
- how data can be shared and remain protected,
- how companies can prove the use of data to their customers, and
- how customers can take greater control of their data (Braun A., Garriga G. 2018, p.671-672).

In 2018, The UK Institute of Business Ethics published an article discussing fundamental values and principles for the use of AI in business: accuracy, respect of privacy, transparency and openness, interpretability, fairness, integrity, control, and impact (IBE 2018). A literature review demonstrates that a number of ethical issues are being discussed within the academic community. These include autonomy, control, manipulation, privacy, users' knowledge, responsibility, trust, and biases (see below). This section will therefore present a literature review of the ethical and societal issues arising from the use of SIS technology in CRM practices.

The literature review was carried out through a combination of online search using generic engines such as Google and Google Scholar, and discipline-specific search engines on websites such as PhilPapers.org and the Philosophers' Index. The bibliographic references of elected papers were then used to locate further literature. Generic searches on Google also provided links to trade publications and websites that were a further source of background information.

2.1. Autonomy, Control and Manipulation

There is a concern among some authors that the autonomy of customers is being undermined through the employment of data analytics. Weston questions whether data analysis techniques are able to measure virtue, cautioning that such analytics are not a neutral tool or measurement: they can expand, constrain or alter people's choices and behaviours, each of which has an influence over the user. He suggests that data analytics treats individuals as already having made or being inevitably about to make certain choices, often with a moral component (Weston 2016, p.38 - 40), but challenges this by suggesting that virtue is "too broad and flexible to be measured" (ibid, p.33). Weston demonstrates that predictions can be a way of giving strong recommendations towards choices and desires, as well as a means to follow and pressure customers around the Internet, leaving them with less autonomy to decide for themselves. Weston's arguments suggest that there are two sides to data predictions: the accurate prediction of a desire may at one and the same time involve the constraint of choice (ibid p. 37-38).

Boyd and Crawford (2012) argue that design decisions determine what will be measured for analysis. This implies that the designers of the analytics systems are making decisions, whether they realise it or not, about which attributes and variables will be counted and which will be ignored. As a general reflection on the design of data analytic systems, this has an impact on the design of such systems used for CRM.

Harrison and Grey (2010) have exposed a correlation between consumer debt and financial institutions' access to information. The authors show how a rise in consumer debt occurred at the same time as the development of complex marketing profile methods that included neural networks and predictive models to target consumers (Harrison and Grey 2010, p. 437). They explain how models that predict a consumer's likelihood of bankruptcy are used to evaluate the profitability of a client, instead of preventing consumers from making harmful financial decisions. For example, new SIS practices can target people who are financially vulnerable and therefore more susceptible to take out a loan (ibid, p.438). Based on these insights, the authors argue that current consumer policies are insufficient to protect susceptible consumers from new direct marketing techniques that use customers' information to exploit and manipulate them (ibid).

Hence SIS technology generally, and by extension that used in CRM practices, has the potential to restrict choice and modify the behaviour of customers. This amounts to the possibility of restricting autonomy and controlling some consumer choices.

2.2. Privacy and Knowledge

Internet access using platforms such as Google, Facebook, or Twitter allows for personal information to be disclosed to the platform and other websites, even if customers do not want to reveal this information. Therefore, privacy issues are a significant concern for CRM practices:

"people unknowingly and unintentionally are communicating personal data to someone else. For marketers Big Data is a powerful weapon for capturing consumer data directly, indirectly, unobtrusively, with and without permission and participation" (Moorthy et al, 2015, pp. 92-93).

Moorthy et al. mention the well-known example of Target, a company which developed an algorithm to find pregnant women based on users' previous activities online (ibid p.92; see also Duhigg, 2012), and the use of facial recognition in social networks to identify people in dating sites (ibid p. 93). Similarly, Braun and Garriga (2018) demonstrate the challenges of using data analytics and explain how anonymous data can lead to uncovering individuals' identity (Braun A., Garriga G. 2018, p.666). Data anonymity is no longer sufficient because by enriching previously anonymous data with external or historical data, personal information may be reconstructed by, for example, finding a person's location hourly by analysing different entry points (De Montjoye, et al. 2013).

Ghosh and Moorthy (2015) also argue that the automation of marketing practices reduces transparency such that the opportunity of exposing sufficient knowledge to customers for informed critique is reduced. For example, the cookie consent procedure introduced by the European Parliament (EU Parliament, 2002) is not enough for a new user to understand the complex mechanisms of data gathering and what a company may be using those data for (ibid, p.93). Data can be stored for longer periods of time and might be put to different purposes. In addition, the authors emphasize that there are important risks to security breaches, such as credit card fraud, given that the data are generated from multiple and different points, rendering them difficult to secure (ibid). Similarly, Braun and Garriga (2018) affirm that the nature of Big Data is to store the data for later use despite often not knowing what that will lead to, which can lead to consumers being uninformed about data usage (Braun A., Garriga G. 2018, p.671).

2.3. Informed Consent

A further challenge to the collection and use of data for CRM and elsewhere is the possible lack of informed consent given by the consumer for data to be used (Foster and Young, 2011). Data may have been given initially for a particular reason, and yet, as noted above, this reason may be replaced by other interests at a later date. In such cases the company may hold the data but not have received informed consent for its use to the latter end. In the case of CRM, the data is collected by the company as customers subscribe to services, but customers may not always consent to having their data analysed for insights or profiling. Even when consent is given, as for instance in the case of store loyalty cards, the apparent means of gaining consent may consist of merely ticking a box to say that you agree to the terms and conditions. However, it is widely accepted that very few people ever read these terms and conditions, and as such the validity of that consent is questionable.

The problem of consumers not reading these terms and conditions to which they give consent is heightened when companies feel the need to protect their terms and conditions in legalistic jargon to avoid class action lawsuits. In such cases, even when a customer attempts to engage with the terms and conditions they may find that they are unable to understand these.

While the centrality of informed consent is well established in some fields such as medicine and academic research, it is less so in marketing. Prior to the introduction of the General Data Protection Regulation



It is widely accepted that very few people ever read these terms and conditions, and as such the validity of that consent is questionable.

(EU Parliament, 2016) and in areas outside the jurisdiction of the EU, a response sometimes raised is that there is no harm involved in the collection and use of such data for purely marketing purposes and so consent is less important than in the aforementioned fields (Hill, 2014). Yet the reason for gaining informed consent from customers, or indeed anyone, is both to limit harm and to respect the autonomy of the individual to participate (Beauchamp, 2009; Manson and O'Neill, 2007).

2.4. Bias

Concerns of bias entering into AI and ML have been growing since at least 2010, and have been well documented by Cathy O'Neil, amongst others (Mittelstadt et al., 2016; O'Neil, 2016). Despite surface assumptions that computers are unbiased as they do not recognize e.g. skin colour or gender, increasing research has been conducted evidencing the potential for the outputs of automated systems to be prejudiced against certain groups of society (Macnish, 2012). This may come from ignoring culturally-specific practices such as clothing choices or walking behaviour, or from drawing understandings of the norm (from which any deviance is recognized by the automated system) from dominant cultures.

Within CRM this might lead to certain groups of society being either ignored, or targeted for particular attention, for no reason other than that the determining program was biased. Ultimately this can lead to legal issues if some groups receive too much or too little attention and respond negatively towards the company as they perceive this to be discriminatory.

An example of this would be when a high-end store uses a loyalty card to maintain contact with regular customers. Given the nature of the store, regular customers are likely to be more wealthy than average. To maintain good customer relations, customers with loyalty cards are offered benefits to "thank" them for their loyalty. These might come in the form of free drinks at the in-store bar, special viewings of sale items, or exclusive savings. In this way, regular (wealthier) customers end up paying less for items in the store than irregular (poorer) customers, potentially exacerbating wealth disparities in society.

An alternative example is that of searching for hotels on an Apple computer or a Windows computer. According to a Wall Street Journal article in 2012, the hotel search engine Orbitz would steer Apple users towards pricier hotels on the assumption that a person who used an Apple was wealthier than one using Windows (Mattioli, 2012). In this case, price discrimination is taking place with a lack of transparency in such a way that people are benefitting from (or being penalised for) their perceived wealth.

2.5. Responsibility and Trust

The unequal power relationship between companies and consumers creates new concerns of accountability, and data ownership (Braun A., Garriga G. 2018). Thus, responsibility for the data is a key concern; for example, the credit risk based on social network profiles has been proven to be inaccurate (ibid p. 667). Data protection and company responsibilities are important for any organization that runs a business built on trust, in which frameworks such as privacy by design are necessary. The following recommendations have been made for business through Privacy by Design (Braun A., Garriga G. 2018, p. 672-673):

- Data sharing with the authorization of the owner (consent) of the data for a specific time frame and for specific purpose;
- Data limits for the purpose of the request;
- Not using data against customers, data should be used for the only purpose established between the owner and the business at the moment of applying data services;
- Confidentiality and data not to be shared with third parties;
- Necessity and proportionality in which business should only store and process data that is necessary for its services and products.

3. Case Study: a Telecommunications Company using CRM SIS

It is important to evaluate whether the ethical issues raised in the literature correspond to those addressed by practitioners. In order to do this, this section focuses on Elisa, a telecommunications company in Finland, and its use of CRM SIS in practice. Elisa uses SIS technology in online marketing practices to improve productivity and reduce churn. It is a telecommunications, ICT and digital services company operating mainly in Finland and Estonia that provides environmentally sustainable services for communication and entertainment, and the tools for organizations to digitalize their operations and improve productivity (Elisa, 2017a). Background research about the use of SIS technology by Elisa was conducted, and an Elisa staff member interviewed. The staff member is responsible for data analysis as part of the group which handles data security and privacy issues.

The interview was conducted in October 2018, at Elisa's Headquarters in Finland. During the interview, the uses of SIS were discussed, and the most fundamental issues corresponding to this technology were reviewed. The qualitative analytics software tool (NVIVO) was used to categorise, define, and evaluate the content of the interview. The interview conducted at Elisa was then segmented and categorised within these nodes, which were analysed to produce this report.

3.1. Description of SIS technologies being used in Elisa

Elisa serves more than 2.8 million customers who account for over 6.2 million subscriptions. The company has become a market leader and presents itself as a pioneer in new network technologies and innovations, such as 5G. Elisa cooperates with Vodafone and Telenor, among others, to enable global services. The company is listed on the Nasdaq Helsinki Large Cap with approximately 190,000 shareholders. In 2017, revenue was 1.79 billion euros, and the company employed 4,700 people in 13 countries (Elisa, 2017a).

Among the regional competences of the group dealing with data analytics, there are three aspects: cybersecurity development, video conference and contact centers (Elisa, 2017b). In addition, Elisa also works with different operational models and subsidiaries such as Elisa Videra, Elisa Applesiini, Enia Oy, and Elisa Estonia. As an example, through Elisa Vidiera, the company has introduced "Hummingbird" (Elisa, 2018), a system designed to monitor and manage assets (customers) and infrastructures; the data it retrieves goes to the study of performance and trending. The principles included in Hummingbird are: real-time advice and interfacing, Big Data management, IoT Device management and control, process and workflow automation, abstracted visualization, and machine learning.

The interviewee explained that the application of SIS is simple: it mainly refers to rule-based systems that enable the handling of customer data to improve systems and services. The purpose of

the technology is network optimisation and the unification of customer identification across platforms. Elisa creates a common digital identity (ID) for a user from different databases to a common master ID, which helps to identify a person in as many ways and places as possible. This is possible through the improvement of machine learning (ML), where Elisa employs data-scientists to create matching algorithms, and the “Aison” product, which is an ML automatic optimization network that helps to, for example, reduce phone calls to customers by finding how likely a customer is to answer their phone call when Elisa is conducting outbound calls. Thus, while accuracy is important, for Elisa better processes and more suitable solutions for customers are needed.

Elisa is also working with AI, where a number of different experiments have been tried, such as reducing customer-care contact. Currently Elisa is very good at estimating whether the customer will make contact again: in the case of billing, for example, the company has found that a typical customer will generally make contact after seven days. Moreover, Elisa uses large datasets to determine the profitability of a subscription package when matched to a particular customer. This then enables the company to avoid being “gamed” by customers. It has also implemented a chatbot, which is a text-based machine operator, by which customers communicate with a machine instead of talking with a human. The chatbot is an option for customers who go online to engage with the company, to filter people whose problems can be resolved relatively easily from those whose difficulties require a human to engage with. When it is used, the chatbot is always displayed to be a robot, so there is no deception on the part of the company in pretending that customers are speaking to a person when they are not. Furthermore, customers are given the choice whether they would prefer to speak to a person or a chatbot, so consent and personal choice are respected. The benefits of using chatbots in this way are that they free up customer support to focus on more challenging issues while the automated system can resolve relatively straightforward issues.

The algorithms used by Elisa allow for pricing decisions to be made based on modelling, which create assumptions about customers. The interviewee explained that customers are treated differently if, for example, a customer has a higher mobile score. However, the interviewee also held that Elisa does not engage in price-discrimination. In the future, the interviewee noted, modelling scores could become a tool to find the optimal price to keep a customer subscribing.

Elisa operates in an industry where the tools of the future are built through continuous development, innovation and cooperation between stakeholders in different fields. For this reason, the company are also closely involved in research projects and startup activities in the industry. The interviewee explained that the company is looking for future projects such as voice-recognition to identify customers and save time in gaining customer data in a phone call. While it is relatively easy to recognise a person online, it is not as simple within a 30 seconds call. Hence Elisa are looking into the storage of voice-samples from customers, from which it will be easier for the customer to be recognized instantly while talking with an Elisa agent. In addition, the interviewee considered the benefits of the possible use of cameras on set-top boxes (STB) to ensure that a person watching TV is not underage.

Table 1

Description		Organisation 1	
Organisation		Elisa	
City		Helsinki	
Sector		Telecommunications	
Name		Interviewee	
Length		123 minutes	

3.2. The Effectiveness of Using SIS for Elisa

The effectiveness of SIS for Elisa relies on its understanding of the reasons for Elisa's "churn score": the number of customers ending their subscriptions. The aim of Elisa's model is to further increase customer orientation and cost-efficiency. For example, the interviewee explained how Elisa asks customers for consent to combine their browsing data with CRM data, which enables Elisa to know if they have a problem beforehand from the browsing behaviour, for example, if they added something to a basket but they have not finished the purchase. In addition, if a customer bought a mobile router from Elisa but the customer is browsing that router online, it is probably because they do not know how to use it.

SIS has also been useful in saving time for customers, keeping customers interested in subscribing to Elisa, and even finding criminal behaviour. It is therefore evident that the use of SIS brings numerous business and customer benefits. However, the company has also faced problems such as the unification of identities: the interviewee stated that there are 11 million different customer accounts, which is greater than the population of Finland. Given that the majority of Elisa's customers are Finnish, the interviewee saw it as imperative that the company improves customer identification across different systems such that each individual entity (person or company) has a unique identity.

4. Ethical Analysis of CRM Using SIS

The interview conducted at Elisa and the background research highlight a number of ethical issues as a result of using SIS technology in CRM practices. These issues widely reflect those found within the literature as discussed in section 2 of this paper. There is therefore a great deal of correlation between academic understanding of the issues with those working in the industry. There is also a relation between the issues faced with CRM technology and the difficulty of dealing with these problems. For example, the power and the potential of gathering data affect the consumer in ways that might have not been predicted. This is a concern which the industry, including Elisa, agree upon but can find no easy solution. Questioning how much quantity of data is necessary to store is a challenging and complex question to answer effectively. Thus, there is a need to start the dialog between the ethical and technical fields.

4.1. Intrusion and Regulatory Differences

Elisa is able to ask customers if they can combine their browsing data with CRM data, which enables identification of a problem from their browsing behaviour. This, as the interviewee explained, can be very intrusive. However, Elisa seeks consent from customers and the terms and conditions are visible on the website. The interviewee pointed out that tracked browsing behaviour relates only to that on Elisa's own website, and not data gathered from other websites or third parties like Google. However:

"The question still remains as to what kind of benefits the user gets out of it." (The interviewee)

The interviewee also argued that Elisa does not need to store excess information beyond that which is already being used.

"Thinking from customer's perspective: if something doesn't benefit the customer, then there's no point doing it either" (The interviewee)

Elisa uses data for modelling in order to find the products that a customer is most likely to buy. In this way, the interviewee argued, the service level becomes much better. The interviewee also discussed the possibility of storing data even if it is not useful, just because in the future it might be. In China, the interviewee explained, the usefulness of data gets to a different level. Chinese data collection tends to be more intrusive than European, so there is a need to assess the cultural and legal parameters of different markets.

The interviewee mentioned the difference between the impact of GDPR in Europe and the situation in other countries, where GDPR does not apply. Depending on the country and the culture, laws are different in a way which influences competitive advantage. For example, it would be comparatively easy for a company based and operating outside of the EU jurisdiction to develop a dataset that would be unethical to produce in Europe. On the basis of this dataset, the company could then develop a highly effective SIS which could then be sold in Europe. This would be economically advantageous to that non-EU company, provided no personal data collected in this manner ever entered the EU. The interviewee felt that, particularly in the light of GDPR companies in Europe both have to and should protect the privacy of European citizens, but that it is incumbent on the EU Parliament to make sure that those companies can continue to compete in the international market, and especially with different parts of the world which espouse different ethical values. Therefore, questions need to be raised about the possibility of the EU placing restrictions on the sale of SIS products which cannot provide evidence of ethical development.

4.2. Privacy and Security

As noted above, privacy issues are a concern, as is the lack of awareness that people have about certain devices, such as mobile phones and smart TVs, being recorded. The interviewee explained that there have been suggestions of putting cameras and microphones in set top boxes, which would invade the privacy of users' homes. In addition, the interviewee pointed out that it is currently possible to gather and analyse TV watched based on subtitle data without the need to carry out video or audio analysis. However, any algorithmic categorization of people based on content

watched will prove difficult to use in predicting behaviour as two very different people can watch similar programmes on TV.

The interviewee further argued that GDPR can serve to raise awareness about the importance of privacy:

“[GDPR can encourage] an awareness among people towards asking what data is being collected from my behaviour? How much data does Facebook (for example) have from me and how much benefit is there in that for me?” (The interviewee)

4.3. Bias and Manipulation of Data

The interviewee argued that ethical concerns in physical systems are relatively easy to recognize, but with digital systems and algorithms an entire system can become biased in a way that is difficult to recognize, for example in cases of gender discrimination. Machine learning systems (MLs) learn from what humans teach them, however many people make the assumption that the information provided by an automation system is correct and unbiased; people trust these systems even if they are proven to contain false positives or false negatives.

Furthermore, the manipulation of customers is possible through the lack of transparency in how these systems function. Informed consent is an important issue, as noted in the literature review, but there is often a lack of clarity on exactly what informed consent allows in particular cases. The interviewee expressed concern about reports on the behaviour of Cambridge Analytica and fake news, and questioned how to educate people in a way that they become aware of this type of manipulation.

“this should be a part of the education, even if people understand much more how this manipulation is taking place nowadays, to recognize when they are being manipulated is a valuable skill” (The interviewee)

This also shows the need to increase awareness amongst the general public, as individuals should be more capable of identifying when they are being manipulated. Furthermore, the interviewee affirmed:

“Democracy will be broken as long as people don't know when they are being manipulated” (The interviewee)

The interviewee expressed how they personally worries about an increasingly Orwellian society and all the surveillance that could be carried out with the kind of data Elisa collects, particularly if governments have access to this data. The interviewee held that in China the public knows that surveillance is taking place; in contrast, in the Western world most people do not know really what surveillance is being performed, nor who is conducting it. However, the interviewee did not produce any evidence to support this claim.

4.4. Responsibility and consent

During the interview the issue of responsibility was raised, in particular the consideration of who has responsibility for collecting data, overseeing that data collection, and informing the public as to what happens to the data:

“Should it be related to individual education or corporate responsibility?” (The interviewee)

The interviewee mentioned that Elisa has public policies for handling customers' data; a code of conduct (Elisa, 2015) and have trained data scientists in this area. In the company it is possible to download the personal data that is stored for each individual subscriber as well as managing the consent from customers. This relates to the company's responsibility. The interviewee argued that Elisa can always do better at informing customers, analysing how well a customer has read and understood the consent. As an example, the interviewee mentioned the Google-inspired mindset of “don't do evil”. The interviewee also felt that governmental organizations should be far more regulated than is currently the case.

4.5. Transparency and the company's vulnerability

It is frequently difficult to make algorithms public, and most customers would not have the ability to understand those algorithms or the input data needed to run them. Furthermore, the algorithms change quickly and models are constantly being updated. From this, one can see how the notion of public "acceptance" of certain algorithms does not really work.

The interviewee argued that for a company, it can be the case that the more open you are, the more vulnerable you are. From a financial perspective, the company has created a model using data to determine, for example, how profitable a customer is. However, Elisa is not yet able to utilize that data to make decisions based on algorithms. Nonetheless, traditional rule-based systems render it easier for customers to game the system, giving them more power and control over the company's offers. This suggests that as regards new CRM practices it would clearly be in the company's interests that the algorithms not be transparent. As the interview said:

“we might be there on a couple of years, and this might affect the capacity of people to use that in their benefit, and the company will be less vulnerable” (The interviewee)

It was argued that GDPR has raised general awareness of data-related privacy issues and led to discussions of personal data collection. It has encouraged people to question what is being collected and why. As a result, the organisational policies in place to address the use and handling of customer data have been made transparent to the user, who can request data from the Elisa website. Similarly, the company's code of conduct (Elisa, 2015) is also available on the website. The following values are included in the code of conduct: consumer orientation, responsibility, renewal, result orientation, and collaboration. The website also mentions the importance of maintaining the trust of the customer, and the importance of confidentiality in managing customer data. However, this doesn't always sit easy with the problems raised above regarding the desired opacity in at least some employment of algorithms as well as the challenge of codes becoming out-dated.

5. Conclusion

There is a need to protect customers from being exploited and misguided through data manipulation and analysis. New advances in CRM practices and data technologies bring social benefits, but also ethical issues that must be examined. This case study demonstrates how companies are using SIS in CRM strategies and their social and ethical implications. The main purpose of this case study was to uncover which ethical issues arise in the use of SIS in CRM. Based on the literature review, the

following issues were identified: autonomy, control, manipulation, privacy, knowledge, informed consent, bias, responsibility and trust.

Table 2

Literature Review	Interview
Autonomy	Autonomy
Manipulation of people	Manipulation of people
Privacy	Intrusion
Knowledge	Lack of knowledge by customers
Bias	Bias
Responsibility	Responsibility
Trust	
Informed consent	
	Different ethical values globally

The interview conducted at Elisa offered a recent perspective on the real-world applications of data management, and also addressed these issues; this case study raises a number of concerns with SIS in CRM:

- 1) intrusion and questions over the usefulness of data
- 2) issues of manipulation and the lack of customers' autonomy;
- 3) the potential for biases in CRM analysis because it is not value-free;
- 4) the cultural differences of ethical issues in different countries;
- 5) the lack of knowledge and awareness by the customer regarding the collection and use of their information; and
- 6) the necessity of companies taking responsibility for data collection and use.

One category that was not mentioned in the literature but was in the interview is that of cultural differences in an international setting. This relates to the fact that there are different laws in different countries, and what is considered to be ethical also changes, which has implications for competition in the international market. Thus questions regarding the potential ongoing implications of international policies and laws are worth considering. This is of particular concern regarding cases where non-European countries may collect data and develop algorithms. In this way, algorithms may be designed and developed outside the EU in a manner incompatible with European regulations such as GDPR. Nonetheless, as explained above, the algorithms could then be employed in Europe in competition with European-developed algorithms. The corporate concern, at least in this instance, is hence that European companies will be unable to develop competitively powerful algorithms, given the limitations on data collection resulting from GDPR. This has long-term implications if it means that unethically-developed products will eventually take over the market due to their effective superiority.

The power and potential of CRM data gathering lead to a variety of ethical issues. Overall, there is a need to address ethical issues in the technical sector and the importance of companies' responsibility in this vastly changing CRM area. The literature review demonstrates that there are questions that arise during the case study which have not been considered in academia, due to the novelty and difficulty of these practices.

5.1. Limitations

There is a dearth of literature specifically addressing ethical issues arising from SIS use in CRM. The focus in applied ethics has tended to be towards social media and insurance uses of algorithms, but CRM in a more general context has not received the attention it merits. Much of the research providing the background literature review was drawn from papers discussing ethical challenges

with SIS in general rather than specifically in cases of CRM, and there are few CRM-related examples. While the interview has raised new ethical issues not covered in the literature, it only engaged with one interviewee from one company. The insights gained above are significant, but they could be supported or challenged by engaging with further interviewees and in other companies.

5.2. Contribution to Knowledge

The research outlined in this report brings several contributions to the state of knowledge regarding the use of SIS in CRM practices. This case study not only offers an addition to current literature and business practices, but also a study for policymakers with new insights into these developing technologies.

This case study offers a literature review of the most pertinent ethical, social and legal issues of CRM. It also presents an interview with an employee working in CRM for one of the largest telecommunications companies in Finland. The interview demonstrated that the academic literature largely raises issues of which practitioners are aware through day-to-day involvement with SIS.

One element of particular concern for the interviewee which has not been explored in depth in the academic literature is the global element of ethical values when it comes to developing SIS. There is a real concern that those companies which develop SIS in a more ethical manner (by, for instance, adhering to laws such as GDPR) may suffer from this. While this should not be a concern in the short term, it may lead to the eventual replacement of those companies by others who are able to compete through not following (and not seeing the need to follow) the same ethical restrictions.

5.3. Implications of this Report

This report can have implications for the development and furthering of CRM theory and knowledge.

The interview also has practical implications; given that it involves a company on the cutting edge in their field. It brings new ethical perspectives to bear on the limitations of CRM. It is hoped that the case study will offer ethical insights to the current field that can be implemented.

5.4. Further Research

This case study is based on a single interview with a single company. While the information gained from that interview is insightful, it is clear that further interviews should be held with other businesses. These would help to determine whether the issues raised here are shared more widely or are unique to the company interviewed, or indeed whether there are other relevant ethical issues not explored here.

It would be valuable to pursue the concern that GDPR and other European regulations place European companies at a competitive disadvantage relative to non-European companies, who are able to collect data (and hence develop algorithms) with fewer restrictions. If this is the case then work should be carried out to determine how best to protect European companies from being harmed for acting in an ethical and respectful manner.

This case study has also shown that the nature of CRM technologies is in a state of continuous development. Additional developments will continue in the future, such as algorithms, AI and ML, and further ethical analysis will be required to monitor their implementation in CRM

practices. To this end, there is a need for ongoing dialog between the ethical community and the CRM community as to which business practices should be pursued in the future.

6. References

- Beauchamp, T.L., 2009. Autonomy and Consent, in: Miller, F., Wertheimer, A. (Eds.), *The Ethics of Consent: Theory and Practice*. OUP USA, Oxford ; New York, pp. 55–78.
- Blázquez, M., 2014. Fashion shopping in multichannel retail: The role of technology in enhancing the customer experience. *Int. J. Electron. Commer.* 18, 97–116.
- Braun, A., & Garriga, G. (2018). Consumer Journey Analytics in the Context of Data Privacy and Ethics. In *Digital Marketplaces Unleashed* (pp. 663–674). Springer, Berlin, Heidelberg.
- boyd D. & Crawford K., (2012). *Critical Questions for Big Data*. Information, Communication & Society, Routledge 15:5, 662–679, DOI: 10.1080/1369118X.2012.678878
- Boerman, S.C, Kruikemeier, S., & Zuiderveen Borgesius, F.J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3), 363–376. doi: [10.1080/00913367.2017.1339368](https://doi.org/10.1080/00913367.2017.1339368)
- Cadwalladr, C., Graham-Harrison, E., 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*.
- Cambridge Analytica, 2017. Cambridge Analytica. URL https://capolitical.com/?_hstc=163013475.3e49f3d22529e528b7209670352a2cae.1543235451820.1543235451820.1543235451820.1&_hssc=163013475.9.1543235451821&_hsfp=2315517664 (accessed 1.4.17).
- Chen, I. J., & Popovich, K. (2003). Understanding customer relationship management (CRM) People, process and technology. *Business process management journal*, 9(5), 672–688.
- Crawford, K., 2013. The Hidden Biases in Big Data [WWW Document]. Harvard Business Review. URL <https://hbr.org/2013/04/the-hidden-biases-in-big-data> (accessed 1.4.17).
- De Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific reports*, 3, 1376.ISO 690
- Dubois, L. (2015). *11 Best Web Analytic Tools*. Retrieved from: <https://www.inc.com/guides/12/2010/11->
- Duhigg, C., 2012. How Companies Learn Your Secrets. *The New York Times*.
- Ebeling, M., 2016. Healthcare and Big Data: Digital Spectres and Phantom Objects. Springer.
- Elisa, 2018. Introducing Hummingbird: More than just monitoring [WWW Document]. URL <http://elisavidera.com/news/introducing-hummingbird-more-than-just-monitoring/> (accessed 12.4.18).
- Elisa, 2017a. On Elisa [WWW Document]. URL <https://corporate.elisa.com/on-elisa/> (accessed 12.4.18).
- Elisa, 2017b. Operational model and subsidiaries [WWW Document]. URL <https://corporate.elisa.com/on-elisa/operational-model-and-subsidiaries/> (accessed 12.4.18).
- Elisa, 2015. Elisa Code of Conduct [WWW Document]. URL <https://corporate.elisa.com/attachment/content/Elisa-Code-of-Conduct-2015.pdf> (accessed 12.4.18).
- EU Parliament, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L.

- EU Parliament, 2002. Directive 2002/58/EC [WWW Document]. Off. J. 201 31072002 P 0037 - 0047. URL <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML> (accessed 1.22.19).
- Enchautegui, M.E., 2013. Nonstandard Work Schedules and the Well-being of Low-Income Families (No. Paper 26). Urban Institute, Washington DC.
- Foster, V., Young, A., 2011. The use of routinely collected patient data for research: A critical review. *Health* 16, 448–463. <https://doi.org/10.1177/1363459311425513>
- Harrison, P., & Gray, C. (2010). The ethical and policy implications of profiling ‘vulnerable’ customers. *International journal of consumer studies* , 34 (4), 437-442.
- Hailwood, J., & Gottlieb, D. (2003). U.S. Patent Application No. 09/972,277. ISO 690
- Hill, K., 2014. Facebook Manipulated 689,003 Users’ Emotions For Science [WWW Document]. Forbes. URL <http://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/> (accessed 9.24.14).
- IBE (2018). *Business Ethics and Artificial Intelligence*. [online] Ibe.org.uk. Available at: https://www.ibe.org.uk/userassets/briefings/ibe_briefing_58_business_ethics_and_artificial_intelligence.pdf [Accessed 20 Oct. 2018].
- Injazz J. Chen, Karen Popovich, (2003). Understanding customer relationship management (CRM): People, process and technology", *Business Process Management Journal*, Vol. 9 Issue: 5, pp.672-688, <https://doi.org/10.1108/14637150310496758>
- The interviewee. Elisa, “Interview”, Finland, 10/03/2018.
- Macnish, K. (2018). *The Ethics of Surveillance: an introduction*. Routledge: London.
- Macnish, K., 2012. Unblinking eyes: the ethics of automating surveillance. *Ethics and Information Technology* 14, 151–167. <https://doi.org/10.1007/s10676-012-9291-0>
- Manson, N., O’Neill, O., 2007. *Rethinking Informed Consent in Bioethics*. Cambridge.
- Mattioli, D., 2012. On Orbitz, Mac Users Steered to Pricier Hotels. *Wall Street Journal*.
- Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S., Floridi, L., 2016. The ethics of algorithms: Mapping the debate. *Big Data & Society* 3, 2053951716679679. <https://doi.org/10.1177/2053951716679679>
- Moorthy, J., Lahiri, R., Biswas, N., Sanyal, D., Ranjan, J., Nanath, K., & Ghosh, P. (2015). Big data: prospects and challenges. *Vikalpa* , 40 (1), 74-96.
- Ngai, E. W., Xiu, L., & Chau, D. C. (2009). Application of data mining techniques in customer relationship management: A literature review and classification. *Expert systems with applications* , 36 (2), 2592-2602.
- Nguyen, B., Simkin, L., & Canhoto, A. I. (Eds.). (2015). *The Dark Side of CRM: Customers, Relationships and Management* . Routledge.
- Ohm, P., 2009. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review* 57, 1701–1777.
- O’Neil, C., 2016. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown/Archetype.
- Parise, S., Guinan, P.J., Kafka, R., 2016. Solving the crisis of immediacy: How digital technology can transform the customer experience. *Bus. Horiz.* 59, 411–420.
- Robinson, D., Yu, H., Rieke, A., 2014. Civil Rights, Big Data, and Our Algorithmic Future. *Upturn*.
- Soudagar, R., Iyer, V., Hildebrand, V., 2012. *The customer experience edge: technology and techniques for delivering an enduring, profitable, and positive experience to your customers*. McGraw-Hill.

- Weston, H. (2016). Data analytics as predictor of character or virtues, and the risks to autonomy. *International Review of Information Ethics* , 24 (05).
- Winer, R. S. (2001). A framework for customer relationship management. *California management review*, 43(4), 89-105. ISO 690

CS10 – Manufacturing and Natural Resources



Case Study

Ethical Implications of Predictive Risk Intelligence



This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641



Document Control

Deliverable	D1.1 Case Studies
WP/Task Related	WP 1: Representation and Visualisation
Delivery Date	31 January 2019
Dissemination Level	Public
Lead Partner	De Montfort University
Contributors	Tilimbe Jiya, De Montfort University Bernd Stahl, De Montfort University
Reviewers	Kevin Macnish, Mark Ryan, Doris Schroeder
Abstract	
Key Words	Smart information systems, responsible research and innovation, ethics, predictive intelligence, ethics

Revision History

Version	Date	Author(s)	Reviewer(s)	Notes

Executive Summary	3
Introduction	4
1. The use of SIS in Predictive Risk Intelligence	5
1.1 Predictive Risk Intelligence in Supply Chain Management (SCM)	5
1.2 Predictive Risk Intelligence in Insurance	6
1.3 Predictive Risk Intelligence in Finance	6
1.4 Predictive Risk Intelligence in Medicine	7
1.5 Predictive Risk Intelligence in Sustainability	7
2. Ethical Issues with SIS in Predictive Risk Intelligence	8
2.1 Security and Privacy Concerns	8
2.2 Integrity	9
2.3 Transparency and Fairness of Automated Decision-making	9
2.4 Algorithmic Bias	10
3. Prewave: A Company using SIS for Predictive Risk Intelligence	10
3.1 Individuals Interviewed	11
3.2 The SIS used by Prewave	12
3.3 The aims of Prewave in using these systems	12
3.4 The Effectiveness of the SIS	14
3.5 General Impacts of the SIS	15
3.6 Stakeholders of Prewave SIS	15
4 Ethical issues with the SIS used in Prewave	15
4.1 Privacy and Data Protection	16
4.2 Transparency and Accountability	16
4.3 Bias	17
4.4 Trust and Accuracy	18
5 Prewave's Effort to Address the Ethical Issues	19
6 Conclusion	21
6.1 Limitations	21
6.2 Contribution	21
6.3 Implications of the Case Study	22
6.4 Further research	22
7 References	22

Executive Summary

This report presents a case study on the ethical issues that relate to the use of Smart Information Systems (SIS) in predictive risk intelligence. The case study is based on a company called Prewave that is using SIS to provide predictive risk intelligence in supply chain management (SCM), insurance, finance and sustainability. Using Prewave as a case study, this report covers an assessment of the company recognises ethical concerns related to SIS and in what ways it deals with them. To understand some of the ethical implications of using SIS in predictive risk intelligence data was collected through a document review and two semi-structured interviews. The document review included an analysis of the literature on ethical issues with the use SIS in predictive risk intelligence, Prewave's website and case studies. The semi-structured interviews were conducted with two participants from Prewave.

Results from the case study indicate that the main ethical concerns with the use of SIS in predictive risk intelligence include protection of the data being used in predicting risk, data privacy and consent from those whose data has been collected from data providers such as social media sites. Also, there are issues relating to the transparency and accountability of processes used in predictive intelligence. Further, the interviews highlighted the issue of bias in using the SIS for making predictions for specific target clients. The last ethical issue was related to trust and accuracy of the predictions of the SIS. In response to the issues that emerged from the case study, Prewave has put in place different mechanisms to ensure responsible innovation through what they call Responsible Data Science. Under Responsible Data Science, the identified ethical issues are addressed by following a code of ethics, engaging with stakeholders and ethics committees.

The ethical issues identified from the interviews are not any different to those covered in the literature. However, they affirm that the use of SIS in predictive risk intelligence poses similar ethical issues regardless of the sector in which the technology is used. This case study report is important because it provides lessons for the responsible implementation of SIS in industry, particularly for start-ups such as Prewave. The report acknowledges ethical issues with the use of SIS in predictive risk intelligence and suggests that ethics should be a central consideration for companies and individuals developing SIS to create meaningful positive change for society.

The report has some limitations regarding the range of the identified ethical issues. Prewave is a start-up, and its technology is still being developed thus more issues could emerge over time regarding the ethical implications of the technology. Nonetheless, the case study gives a starting point for reflection by revealing some of the current ethical issues, therefore laying a foundation for anticipating on future issues with the use of SIS in predictive risk intelligence and how they could be addressed.

Introduction

The use of predictive risk intelligence through the combination of Artificial Intelligence (AI) and Big Data is reaching new horizons, alternatively known as smart information systems (SIS). SIS are widely used to provide intelligence in many areas predicting risk, such as supply chain management (SCM) (Bendoly, 2016), sustainability (Kant and Sangwan, 2015), medicine (Williams et al., 2018), finance (Xia et al., 2013) and insurance (Baecke and Bocca, 2017). All these approaches involve the use of advanced machine learning techniques that integrate data to deliver predictions of risks affecting the critical elements of enterprises and communities.

One company that is developing such risk intelligence is Prewave. Prewave is an AI spin-off that was created at the Vienna University of Technology through seed financing and investment from IST Cube. IST Cube is a new incubator and accelerator based at the Institute of Science and Technology in Austria, and Pioneer Ventures (TU Wien 2018). Prewave came about as a result of five years of intensive machine-learning research at the university (TU Wien 2018). Prewave's technology aimed to develop an approach towards risk intelligence and management through the use of social media, news data, and supply-chain data and AI.

SIS technologies are advancing at a remarkable rate, and this may lead to many beneficial applications such as predictive analytics. Harnessing this advancement, Prewave uses SIS to suggest predictive risk intelligence for improvements in areas such as supply chain management (SCM), insurance, and finance (WeXelerate 2018). However, the use of such technologies come with some ethical concerns such as data privacy, integrity, transparency and fairness, bias and the accuracy of predictive intelligence. Using Prewave as a case study, this report addresses the research question: *how do organisations working with predictive risk intelligence perceive ethical concerns related to SIS and in what ways do they deal with them?* To address this research question, data was collected through a literature review, two semi-structured interviews with participants from Prewave, and a review of their website and the company's case studies.

In section 2, the report presents a review of the current use of SIS in predictive risk intelligence. Section 3 discusses a range of ethical issues surrounding the use and implementation of SIS in predictive risk intelligence. In section 4, the report describes Prewave and outlines the objectives of using SIS in the organisation. This section also discusses the effectiveness of SIS used in Prewave, before considering the impact of such systems on the organisation. In section 5, the report presents ethical issues that were identified in the use of SIS at Prewave. Following the identification of ethical issues, section 6 presents remedial actions that are used to recognise and address ethical issues in the company. This report contributes to the understanding of ethical issues when using SIS in predictive risk intelligence and supports the discourse that is aimed at addressing those issues.

1. The use of SIS in Predictive Risk Intelligence

The use of SIS in predictive risk intelligence is based on models that are developed using non-conventional approaches such as artificial neural networks⁵⁴ and support vector regression⁵⁵ (Kant and Sangwan, 2015). Such predictive analytical models can be used to identify both long- and short-term risks. Predictive risk intelligence is gaining ground because it leads to better allocation of resources, targeted prevention strategies, and improved decision support (Torous et al., 2018). To this effect, new statistical methods are being developed to optimally utilise existing data and make the most accurate predictions about risk (Kant and Sangwan, 2015; Torous et al., 2018).

Key to the use of SIS in predictive intelligence is machine learning. Machine learning is an AI approach to make predictions by learning from existing data instead of requiring additional programming (Cohen et al., 2014). Machine learning utilises modern computing and mathematical algorithms to build models based on available data sets, in which the model itself can improve with experience (Torous et al., 2018). Using machine learning, SIS are capable of recognising complex combinations of variables that reliably predict an outcome (Hall and Pesenti, 2017; Williams et al., 2018). SIS employs machine learning to analyse large, heterogeneous data sets that are then used to predict outcomes for a wide range of eventualities including risk. For instance, the modelling and predictive capabilities of SIS can be applied in industry and communities, which promotes efficiency and effectiveness of decision-making (Bentley et al., 2018).

The current generation of SIS is particularly suited for augmenting or automating tasks that involve at least some broadly defined predictive function. These cover a wide range of tasks, occupations and industries, from driving a car (predicting the correct direction to turn the steering wheel), diagnosing diseases (predicting its cause), to recommending a product (predicting what the customer will like), or writing a song (predicting which note sequence will be most popular) (Brynjolfsson et al., 2017).

1.1 Predictive Risk Intelligence in Supply Chain Management (SCM)

At the core of the use of SIS in predictive risk intelligence in supply chain management (SCM) is Big Data. The use of SIS carries with it the opportunity to change the SCM design and day-to-day decision-making. Thus, SIS are used to provide predictive intelligence through a range of techniques, resources, tools, and applications, ranging from baseline statistical analyses to advanced simulations (Waller and Fawcett, 2013). This growing combination of resources, tools, and applications has significant effects in the field of supply chain management. Some of the effects include improving forecasting accuracy, reducing costs and gaining better

⁵⁴ An artificial neural network (ANN) is an implied model of the biological neuron to make decisions and conclusions by simulating the human brain's work (Bryant and Frigaard, 2006)

⁵⁵ Support Vector Regression (SVR) is a tool from machine learning that can build a regression model on historical time series data for the purpose of predicting future trends (Xia et al., 2013)

contextual intelligence across supply chain operations, which translate into lower costs and quicker response times to customers (Jeble et al., 2018; Waller and Fawcett, 2013).

SIS are also used to revolutionise supply chain dynamics through data sets, new methods of data science and new applications in the form of predictive analytics (Bendoly, 2016). Some of the methods that are used in SCM predictive analysis harness the potential of social media to provide large datasets (Singh et al., 2018). Using social media in predictive analytics in SCM is prevalent. For instance, SIS are used for data capture at multiple points in the supply chain process in order to determine risks and opportunities. These data may be consumer sentiment data resulting from Tweets, Likes, and product reviews on websites (Singh et al., 2018; Waller and Fawcett, 2013).

1.2 Predictive Risk Intelligence in Insurance

Machine learning (ML) algorithms promise advancements in insurance risk management. Advances in computational power, the increasing amount of available risk data and the quality of data collected have helped SIS develop further when it comes to predicting risk and can therefore help in insurance decision-making processes (Baecke and Bocca, 2017). As is the case with other areas where SIS is used for predictive risk intelligence, the advances in SIS technologies allow ML algorithms to learn patterns in data which are indiscernible to human eyes and predict future risks (Jordan and Mitchell, 2015). For instance, SIS based on these algorithms can automate an expert insurance analyst's work, make routine decisions independently and raise problematic cases for review. As a result of such use of SIS in insurance, valuable expert time can be allocated where it is most needed while keeping the risk assessment up-to-date and available for all of its users. Automatic credit risk scoring systems, based on ML algorithms, are behind most current credit decisions and aid in calculating insurance premiums to cover different types of credit based on the risk of defaulting payment (Louzada et al., 2016).

1.3 Predictive Risk Intelligence in Finance

In finance, SIS plays a significant role in predicting risks and future trends in the financial market, and in support of decision-making in trading financial instruments such as stock (Coyne et al., 2017; Fischer and Krauss, 2018; Geng et al., 2015). Stock market prices are volatile. Wang et al. (2016) suggest that SIS can be used to make predictions in the stock market. It also serves as an early recommendation system for short-term investors and an early financial distress warning system for long-term shareholders. The predictions are made using price data to predict market index direction and stock price direction, and highlight risks and opportunities within the financial market (Fischer and Krauss, 2018; Geng et al., 2015). Therefore, SIS is also used by business owners, investors and policymakers alike to speculate on risks and trading trends (Coyne et al., 2017; Xia et al., 2013). For instance, investors and consumers use social media to share their thoughts and opinions which creates a large

amount of data that can be used for predictions. An example is StockTwits⁵⁶ which is a social media platform used by investors to share information on stock trading (Coyne et al., 2017). Using SIS, such information is employed to understand and predict individual stock prices and determine risks associated with the stocks.

1.4 Predictive Risk Intelligence in Medicine

There is a growing use of SIS in predictive risk intelligence in medicine. For instance, rapid progress has been made in clinical analytics-techniques for analysing large quantities of data and gleaning new insights from that analysis to identify and manage high risk and high-cost patients (Bates et al., 2014; Hamet and Tremblay, 2017). There are several opportunities to use SIS to reduce the costs of health care and to help identify high-risk patients, such as those at risk of cardiac arrest (Cohen et al., 2014; Petersen, 2018; Williams et al., 2018). Also, models based on ML can instantaneously consider the risk of all patients in a hospital and their individual therapeutic preferences (Cohen et al., 2014).

1.5 Predictive Risk Intelligence in Sustainability

Although progress with the use of SIS has largely been limited to areas such as medicine and finance (Keeso, 2015), there is a pressing need to integrate SIS within sustainability. Sustainability (environmental, social and commercial) is an emerging area for SIS applications. For example, some emphasise the need for SIS in the promotion of sustainability to attain business and strategic benefits (Hazen et al., 2016; Mani et al., 2017). Hazen et al. (2016) and Mani et al. (2017) support the need for techniques that can process a large volume of data to gain actionable insights into environmental, social and economic sustainability.

Using SIS to generate insights at both strategic and operational levels is considered crucial for sustainability. Particularly in the supply chain's operation-planning phase, SIS have been used widely to solve problems with procurement, inventory, and logistics (Hazen et al., 2016; Wang et al., 2016). Hazen et al. (2016) and Wang et al. (2016) further suggest that the use of SIS analytics can help predict and avert risks but also create innovative resources which can deliver strategic advantage and sustainability.

Correspondingly, a study by Chopra and Sodhi (2014) showed that the use of SIS in supply chain risk management could avert potential disruptions and help in rapid recovery from disruption. Such disruptions in the supply chain may be caused by various risks including material flow risk, information flow risk and financial flow risk (Chopra and Sodhi, 2014).

In this section, several areas of the use of SIS in predictive risk intelligence were discussed to provide a picture of the state-of-the-art. Despite these positive uses of SIS in predictive risk intelligence, there are related ethical issues, which will be covered in the following section.

⁵⁶ <https://stocktwits.com/>

2. Ethical Issues with SIS in Predictive Risk Intelligence

The use of SIS in predictive risk intelligence raises several ethical issues. During background research into the ethical issues of using SIS in predictive risk intelligence, a number of sources were used. These sources included journals such as Science, and the International Data Privacy Law journal. Also, insights were derived from proceedings from conferences such as International Conferences for Internet Technology and Secured Transactions to further understand the ethical issues with SIS technologies. In coming up with relevant literature, a broad search of keywords using different variations was conducted in databases such as Google Scholar and Scopus. After reviewing these articles, some ethical concerns with the use of SIS in predictive intelligence such as security and privacy, integrity, transparency and algorithmic bias were established.

2.1 Security and Privacy Concerns

Ideally, predictive analytics or predictive intelligence involve linking data from multiple sources with social data to identify trends and provide insights for decision-making. With many new sources of data becoming available, such as data from social media applications, aggregating these data sources to achieve predictive analytics raises privacy concerns and requires new ways to preserve privacy (Bates et al., 2014; Petersen, 2018).

Several of the concerns, such as automated spear phishing⁵⁷ and personalised propaganda⁵⁸, rely on the owners of SIS gaining unauthorised access to personal information about individuals. The risks posed by the use of SIS to security and privacy are exacerbated by poor threat-detection methods that misclassify malicious threats as benign, fail to detect key provocations or involve authentication mechanisms capable of misidentification and misinformation due to data misuse (Gupta, 2018; Horvitz, 2017).

One example that highlighted some of the privacy concerns with SIS was the Cambridge Analytica-Facebook scandal. In 2016 Cambridge Analytica was involved in creating advantages for candidates in elections in the United States of America (USA) and the United Kingdom (UK). Cambridge Analytica, in conjunction with Facebook, was at the centre of harvesting and using personal data to influence the outcome of the US 2016 presidential election and the 2016 UK Brexit referendum. Cambridge Analytica used Big Data and advanced ML techniques to provide a full suite of services to enable highly targeted marketing and political campaigning, which raised concerns with regards to the privacy of those whose data had been accessed (Gupta, 2018; Isaak and Hanna, 2018).

⁵⁷ The fraudulent practice of sending emails from a known or trusted sender to induce targeted individuals or organisations to reveal sensitive information

⁵⁸ Information, especially of a biased or misleading nature, that is not objective and is used to influence an agenda or point of view.

2.2 Integrity

Another ethical issue with predictive risk intelligence relates to a lack of integrity when designing or using algorithms. For many companies, revealing certain information would have a knock-on effect on their business. Therefore, they may compromise the integrity of their processes in order to save their business (Hacker, 2018; Terzi et al., 2015). There is a potential for an imbalance between a business's interests and its moral obligations to other stakeholders. For instance, a company may propose a prediction that may improve particular social conditions around the world, but it may be unclear about its social obligations and to whom it is accountable. In a case where a company's client uses morally unacceptable practices such as discriminatory profiling, there is a much higher likelihood of risk to the company which offers the predictive intelligence if this information is revealed, and so algorithms could be intentionally designed to ignore the practice (TU Wien, 2018).

2.3 Transparency and Fairness of Automated Decision-making

A further concern with the use of AI in predictive risk intelligence is the transparency and fairness of the algorithms used with the intelligence (Wachter et al., 2017a). According to Wachter et al., (2017) this concern arises because SIS use complex and opaque algorithmic mechanisms that can have many unintended and unexpected effects. When it comes to transparency and fairness in the automated decision-making process, such as predictive risk intelligence, users or clients only get a limited idea of why a decision has been made in a certain way, which does not mean the decision is justified or legitimate (Wachter et al., 2017b).

Some scholars, such as Hacker (2018), Horvitz and Mulligan, (2015) and Meira (2017), affirm that when it comes to the use of SIS in making decisions, for instance around risk, there may be a lack of transparency around what data is being used to train decision-making algorithms in the first place. A real-life example of such issues is the case of the Wonga payday lender in the United Kingdom. Wonga obscurely used more than 7,000 data points to assess how likely applicants were to default on a loan (Katwala, 2018).

The Wonga Case: Use of Leaky Data

Wonga was the most high profile and controversial payday lender in the UK which used technologically advanced AI and Big Data techniques to automatically sorting through over 7,000 different data points, to sort borrowers who will repay from those who will not, based on its distinctive method of credit assessment.

According to Joe Deville's study published in Charisma on Consumer Marketing Studies, Wonga was using a variety of leaked data on credit scores, IP addresses, type of browser and time of the day the application is made and applicant News feed on Facebook to predict if a borrower would default. However, it is was not transparent how calculations were made to come up with the predictions. More information can be found via, <http://www.charisma-network.net/finance/leaky-data-how-wonga-makes-lending-decisions>

2.4 Algorithmic Bias

There are also concerns about the reliability of using AI in making predictions. For example, AI can learn bias and prejudicial values when they are present within the dataset, leading to unfair or inaccurate predictions (Barocas and Selbst, 2016; Crawford and Calo, 2016). A lack of reliability in the predictions that are made by the SIS can be introduced when certain data are either included in or excluded from the training dataset (Williams et al., 2018). Due to potential bias in developing algorithms, AI can learn pre-existing inequalities that are present in the training dataset, resulting in a bias towards historically disadvantaged populations (Barocas and Selbst, 2016).

Additionally, data can be manipulated and misinterpreted according to the predispositions of those who are handling and manipulating data for making predictive intelligence (Katwala, 2018; Terzi et al., 2015). An example of such bias is given by Hacker (2018) regarding the use of SIS in predictive medical intelligence. In predictive medical intelligence, the algorithm may reflect existing biases, with certain medical treatments being chosen on the basis of the practising physician's speciality. Such issues highlight the importance of integrating data quality protocols and high ethical standards to mitigate bias and discrimination when using SIS for predictive intelligence (Hacker, 2018).

3. Prewave: A Company using SIS for Predictive Risk Intelligence

One of the companies using SIS in predictive risk intelligence is Prewave. Prewave was incorporated in 2017 and stems from five years of advanced ML research conducted at the Vienna University of Technology. Prewave's technology generates risk intelligence for its clients, derived from worldwide social media and news data. Using Prewave, a leading global logistics provider has successfully integrated a working prototype for SCM applications, and

it is hoped the technology will lead to substantial benefits for other markets, such as sustainability and insurance.

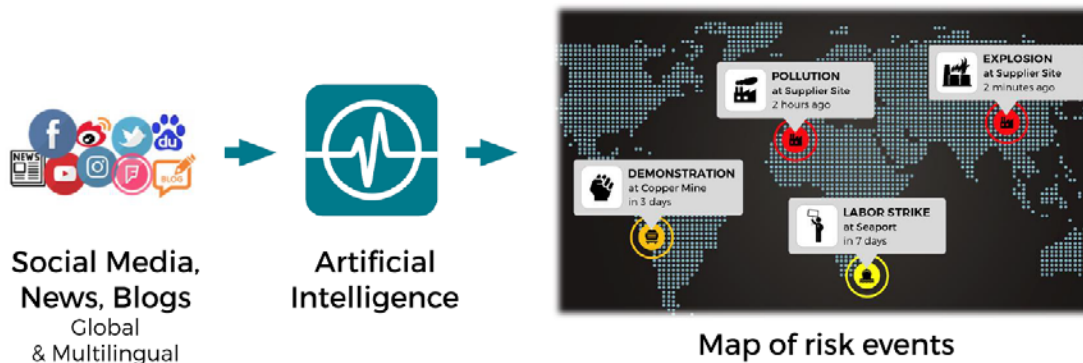


Figure 1: Prowave's operation (Source: www.prowave.ai)

Prowave uses data retrieved from Facebook, YouTube, Twitter and local networks in each country being assessed (such as the Chinese Weibo) to construct a risk analysis profile for companies and establish approximate predictions for their decision-making team (Dax, 2018). The SIS used in Prowave involve constantly learning and evolving AI techniques that can offer relevant, advanced predictions for a vast canvas of potential risks affecting business operations (TU Wien 2018). Prowave develops technologies to predict and detect social events using a variety of external data sources, including social media data.

The data collected were analysed using a thematic data analysis technique which was both deductive and inductive. The deductive themes were derived from the interview questions to begin the analysis process. Using Nvivo qualitative data analysis software, categories were established into different nodes during a two-day SHERPA consortium workshop. Consequently, inductive themes emerged from the interview transcripts to inform this case study report

3.1 Individuals Interviewed

To obtain an in-depth understanding of the ethical issues related to the use of SIS in Prowave, two individuals from the company were interviewed after giving their consent to use their data for publication. The roles of the individuals interviewed included managing the operations of the start-up to controlling data science and business analysis, including marketing. Table 1 shows the interviewees and their roles.

Interviewee	Role in the Prewave	Date of Interview
Interviewee 1	Managing Director	27.09.2018
Interviewee 2	Business Analyst	27.09.2018

Table 1: Interviewee roles in Prewave

3.2 The SIS used by Prewave

The core technology used in Prewave is termed The Prewave Prediction Engine. The prediction engine uses smart information systems that enable the company to detect risk events on a global scale, days and sometimes even weeks before they happen (Prewave, 2018). The predictive intelligence is used to improve decision-making for various application domains and markets, ranging from Non-Governmental Organisations (NGOs) to supply chain management, corporate sustainability, and the insurance industry (Interviewee 1).

The SIS is used to analyse media streams with advanced data analytics technologies. This involves data retrieval from a range of social media sites, which is then analysed by ML algorithms to determine predictive outcomes for clients. The algorithms are trained in a number of languages and can evaluate a wide range of risk factors. Prewave's primary background is the analysis of SCM and logistics, to determine possible supply chain disruptions and identify suitable alternatives, but its analytics have branched out to encompass the identification of insurance risks and business interruptions, as well as establishing issues affecting finance companies and sustainability agendas (WeXelerate, 2018). Prewave offers its predictive knowledge through plugins, application programming interfaces (API), and the Prewave web-based mapping (Prewave 2018).

Prewave used SIS to predict major national port workers strikes across seaports in Indonesia 18 days before they occurred (Prewave, 2017). The cooperative for workers responsible for loading and unloading cargo triggered the strikes because it was dissatisfied of its workers' rights. Using SIS, Prewave was able to detect consistent pre-signals in social media messages and formulated an alert and risk level of impending strikes (Prewave, 2017).

3.3 The aims of Prewave in using these systems

There are several reasons Prewave uses SIS in support of its core business. The first interviewee mentioned that Prewave is a start-up that operates within the IT sector focussing on data analytics. Therefore, the SIS aims to analyse data and provide services to its clients on a range of decision-making processes. Interviewee 1 said that:

'we produce the algorithms and the business model is [that] we actually sell data'.
(Interviewee 1)

This was confirmed by Interviewee 2:

‘Prewave has the ability to extract insights that have the power to change practices in the world of enterprise, social, environmental, ethics and chain of custody intelligence to expose supply chain risk’. (Interviewee 2)

The SIS in Prewave is aimed at understanding real events affecting international supply chains, the discovery of critical elements across the impact value chain, and real-time knowledge for business continuity (Prewave, 2018a).

To encapsulate the aims of the SIS in Prewave, Table 2 shows the areas within the suppliers’ ecosystems where predictive intelligence offers virtual insights.

Area of Supplier Ecosystem	Examples of insights gained from SIS
Social systems	Human and labour rights issues or violations, labour unrest, unfair treatment of workforce, child labour, discrimination
Environmental systems	Environment, health and safety (EHS) violations or concerns, workplace accidents, hazardous materials, waste disposal, pollution
Ethics	Lawsuits, civil charges, corruption, political ownership or influence
Chain of custody	Actions or behaviours that may reveal violations
Additional risk insights	Historically associated risks both human-made and natural

Table 2: Use of Predictive SIS in Suppliers’ Ecosystems (Adapted from www.Prewave.ai)

Prewave is currently piloting the use of systems from the insurance field to identify product risks, using SIS. An example was given by Interviewee 1 in relation to predicting risk for a cosmetics company:

‘if you have a cosmetics company producing shampoo or makeup, and if people are publishing that they get allergic reactions related to that product, that would be a risk that can show up on social media, for example, or in news data....So we focus on early detection, so many other companies do real-time risk monitoring, but we aim to detect the risks even before they happen [...] very quickly in multiple languages’. (Interviewee 1)

In addition to using SIS in predicting a health and safety risk, Prewave also uses it in predictive finance by analysing data:

‘for investors to understand where their money is actually going and therefore make better decisions’ (Interviewee 1).

Similarly, the SIS is also aimed at providing local information on supply chains to help clients know if a supplier is risky to work with, by highlighting if there have been problems with that supplier in the past (Interviewee 1).

In terms of ethics, according to Interviewee 1, the SIS is aimed at highlighting:

‘wrongdoing by structuring unstructured information on a huge amount of issues and using that to blow a whistle in a non-aggressive way that can help the company, help the economy and help all the shareholders and stakeholders around the company’ (Interviewee 1).

To add to this, the SIS that is used in Prewave is aimed at:

‘making data structured and relevant for the right reasons to the right causes in a world with insane amounts of very messy unstructured data’ (Interviewee 2).

3.4 The Effectiveness of the SIS

The SIS used in Prewave is proving to be effective toward its aims and goals. This was suggested by Interviewee 2, who talked about the positive strides that the Prewave SIS is making. The interviewee said that the SIS:

‘has the ability to extract insights that have the power to change practices in the world of enterprise’. (Interviewee 2)

The SIS allows for better decision-making, which means a more informed understanding of what is entailed by certain decisions, the actions that will come from those decisions and any knock-on effects. Therefore SIS has a big role in making decisions that are based on an informed understanding of the issues surrounding risk in insurance, supply chain management and sustainability.

According to the interviewees, the use of SIS in Prewave is so effective that the company is evaluating opportunities in different domains, such as finance. Apparently, the SIS has some good testimonials from users. It was indicated by Interviewee 1 that a client who invested in a company in a different country received a report about potential risks there, and acknowledged that the information was crucial in understanding the problems faced by people living around the client’s company in that respective country.

Despite the effectiveness of the SIS thus far, Interviewee 1 admitted that there is still a need to have a human verification step within the process, considering that the SIS is still being developed. The interviewee further said that there is a need to improve and learn how to calibrate the AI better.

Regarding the maturity of the SIS in Prewave, according to Interviewee 2, the system is in its growth stage, and there is still room for it to mature and be refined so that the processes become more effective and more efficient over time. For example, the website is still being developed to make it more user-friendly and informative to increase online traffic.

3.5 General Impacts of the SIS

The SIS has some positive impacts on society and industry. The target market of the SIS is not localised to a geographical region, but has also shown impact in several parts of the world (Prewave, 2018b; TU Wien, 2018). One of the impact of the SIS has been its capability to detect positive use cases that are used to limit risk in areas that affects local and international economies such as finance and sustainability.

For instance, Prewave is trying to launch a pilot with labour unions in different countries to see if they could use the SIS to predict strikes and help the unions use the latest technologies to know what is going on, and support their members effectively. Interviewee 1 gave an example whereby Prewave provided predictive intelligence on labour unrest and industrial accidents to a Non-Governmental Organisation in Hong Kong. The predictive intelligence provided information that was published in an effort to make the labour unrests and industrial accidents transparent.

3.6 Stakeholders of Prewave SIS

The stakeholders of Prewave's SIS are wide-ranging. Interviewee 2 said that the stakeholders include:

'mother earth, the employees, the communities around the world that we'd extract data from, the public and the investors behind us'. (Interviewee 2)

This shows that potential stakeholders for SIS range from individuals (citizens) to governments. For example, labour unions are interested, along with people from different organisations, NGOs, the investor community, and the general public.

So far, this report has covered the use of SIS in Prewave and its effectiveness towards achieving the organisation's aims and the aims of the different stakeholders. However, despite all the positive impact that predictive intelligence could offer, there are some ethical issues. A number of them have been highlighted in the literature as briefly discussed in section 3 above. The next section outlines the ethical issues that emerged specifically with the use of SIS in Prewave.

4 Ethical issues with the SIS used in Prewave

A number of ethical issues arose from the use of SIS for predictive risk intelligence. Some of the ethical issues that emerged correspond to those that have been covered in the literature with regards to the use of SIS in predictive intelligence in supply chain management,

insurance, finance, medicine and sustainability. The ethical issues that emerged from the two interviews related to privacy and data protection, transparency and accountability, reliability, and finally trust and accuracy of the predictive intelligence. These ethical issues are discussed below.

4.1 Privacy and Data Protection

The first ethical concern that came out of the interviews was to do with privacy and data protection. The use of social media data has many implications for privacy, as has been seen in the case of Cambridge Analytica, which was using Facebook data for predictive analysis (Isaak and Hanna, 2018). With the use of social media data, there is the likelihood that the SIS could have unauthorised access to the personal data of unsuspecting social media users whose data are collected for predictions, which poses a risk to privacy. Considering that the SIS used by Prewave collects a lot of social media data, this poses a concern, especially if there are outsiders such as hackers who could get hold of the data collected and use it for purposes that were otherwise unintended.

The issue of privacy and data protection is also linked to the malleable nature of the techniques used to predict risk intelligence. Despite having security procedures in place, the techniques used in predictive intelligence could have disruptive effects in the flow of ideas, and access to information that results from the advancement of innovation around the information marketplace. This risk is further exacerbated by the interconnectivity of technologies that are used in SIS whereby localised systems are becoming more integrated into larger systems that govern every aspect of people's lives such as social media. Such larger systems are being controlled by multi-national organisations or governments which has a lot of implications on the privacy of the data being collected and stored.

4.2 Transparency and Accountability

From the interviews, the second ethical issue relating to the use of SIS in Prewave is transparency. It was established that the processes used to cultivate the predictive intelligence are not yet transparent. For instance, Interviewee 1 mentioned that:

'[people] understand what we are doing, but they do not know how we are doing it; it's actually our goal, also, to keep that a secret, because that's the only way, and because we can't really ask for a patent, that's what we checked, it's very hard to protect our intellectual property'. (Interviewee 1)

The issue of transparency in this case seems to be a result of protecting the business, which could be argued to be valid for Prewave's survival. However, it is still an ethical concern when there is no transparency in how the data is collected and manipulated. This was also confirmed by Interviewee 2 who said:

‘we actually try to keep it secret [...] which is sometimes a bit of a problem if you want to talk to universities and collaborate’. (Interviewee 2)

To show how the issue of transparency is significant in the use of SIS in Prewave, Interviewee 1 stated that:

‘data providers, for example, Twitter, figured out that we’re using their data and that we’re using it quite actively and asked us if we could provide some feedback on how their data is shipped and so on’. (Interviewee 1)

This shows that the issue of transparency is relevant on both sides of the process, for the data subjects (the public), and the data providers.

The issue of transparency in using the SIS to predict risk intelligence also has implications for informed consent. The assumption is that since the data is public, the data subjects do not clearly object to others using it. This was suggested by Interviewee 1 who said that:

‘so they don’t know that we analyse the data; the data is public, and thereby also considered to be in the public domain and, by publishing their data on the platform, they agree or even ask the platform to publish it’. (Interviewee 1)

Such an assumption is open to scrutiny and has some similarities to the case of Cambridge Analytica mentioned in section 5.1 above.

However, with regards to internal transparency, Prewave reports its activities to its funders and its employees through regular meetings. For example, Interviewee 1 stated that public funding of organisations in Austria triggered a lot of discussion around ethics and human rights, because as a start-up Prewave uses both private equity and public funding, and so there is a need for accountability and transparency to these public organisations where the risks and benefits of the technology are discussed.

4.3 Bias

The third ethical consideration with the use of SIS in Prewave is bias. The issue with bias in the use of SIS can manifest through the selection of clients for predictive risk analysis. Interviewee 1 stated that the company *‘consciously’* selects their clients. This sounds as if there are some preconditions in selecting clients who would work well with the Prewave system. In this case, there is a high chance of bias or predisposition which could have implications on how the algorithms are designed and used.

For example, Interviewee 1 mentioned that the sample to use for predictive intelligence is preconceived to give certain expected outcomes. The interviewee said that there are objectives when picking the sample size, so that samples of potential interest are selected, which could give certain results, as mentioned in the excerpt below:

'... if there is an abnormality, then we would detect it as something that is potentially wrong or potentially of interest, like a corrupt event. If it's said by several people [then] the sample size is ... more objective. Then we can pick it up'.

4.4 Trust and Accuracy

The fourth ethical issue is around trust and the accuracy of the SIS in predicting risk. This may possibly be a result of using misrepresentative data or misrepresenting information, as suggested by Interviewee 1:

'if we paint a different picture to what it actually is in reality, only because the public representation looks like that [...] that's a real issue, and that's a risk that could arise'.
(Interviewee 1)

The interviewee acknowledged that there is a risk with accuracy of the predictive intelligence. If the intelligence is inaccurate, it will have a knock-on effect on the trust of the clients or stakeholders that use such information.

When it comes to using Big Data, Interviewee 2 indicated that accuracy is fundamental because of the influences that surround the data manipulation such as *'data promiscuity'*. Data promiscuity is the desire to mix data for indiscriminate purposes and so has the potential to lead to inaccurate outcomes. Interviewee 2 also stated that with the use of SIS in predicting risk, it is important that the:

'outcomes are more targeted and are a clearer representation of that data that can be used for some sort of betterment'. (Interviewee 2)

The interviewee further said that an accurate identification or a prediction is something that can be used for a good decision, rather than going towards unclear outcomes, therefore:

'[the] problem is finding a clear way [...] to use the data in the best way possible. Have it measurable, visible and tangible in front of you as opposed to just getting caught up in the flood of buzzwords' (Interviewee 2),

The issue of accuracy is also connected to the effectiveness of the SIS when predicting risk. Prewave acknowledges the limitation of the SIS that is used in the company and therefore considers involving human intervention in ensuring accuracy. Interviewee 2 said:

'we need to find out what our clients would tolerate. If they say, okay, they want 99% accuracy and no wrong alerts at all [...] then I think we will always have the last step where a human, at least for some of the cases where our machine says "I'm not sure," needs to make the last decision. So I think it will be hard to eliminate the human totally'. (Interviewee 2)

In this section, we covered some ethical issues that are related to the use of SIS in Prewave. It is fair to say that the company recognises most of the issues that emerged in the literature

review such as privacy, integrity, transparency and bias. To show such recognition, Prewave has put in place some measures to address the ethical issues. These remedial measures are presented in the next section.

5 Prewave's Effort to Address the Ethical Issues

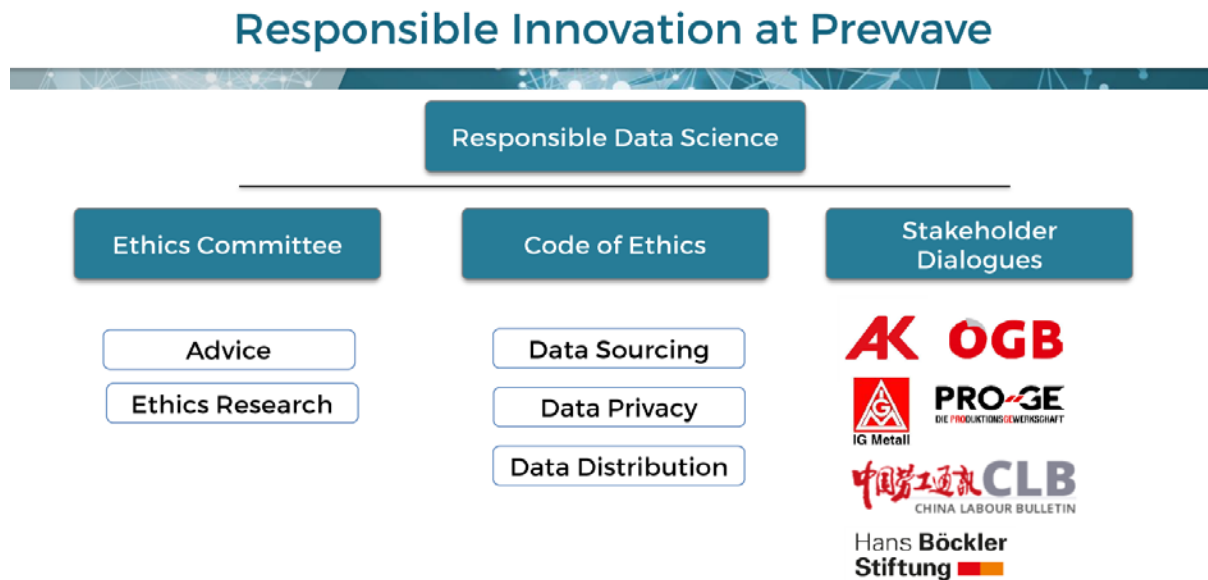


Figure 2: Responsible Innovation at Prewave (Source: www.respect.at)

Prewave recognises that it functions in a time of advancing technology, when data privacy implications are prevalent. In order to ensure that the issue of data privacy is addressed in a way that mitigates the risks connected with data breaches and lawsuits, the company follows Responsible Data Science. Responsible Data Science involves methods aimed at limiting the potential for misuse of personal data and the risk of undermining public trust through fairness, accuracy, confidentiality, and transparency of data use (van der Aalst et al., 2017). Under Responsible Data Science, Prewave aims to adhere to a code of ethics. The code of ethics is aimed at ensuring that the use of SIS in Prewave remains legal, ethical, socially responsible and accountable to different stakeholders (Prewave, 2018c). As pointed out in section 5.3 above, transparency is one of the ethical issues that relate to the use of SIS in Prewave's predictive intelligence business. However, Prewave is aware of the ethical concern and has put provisions within its code of ethics to address it. For instance, it is stipulated in the code of ethics that the company aims:

'to ensure transparency about their activities and what may happen as a result of the data that they provide and that their technologies will provide a benefit and value to society while minimising risk' (Prewave, 2018c).

Prewave also has a data privacy and protection plan which covers the use of lawfully obtained publicly available or proprietary data; aggregation and anonymisation of meta-data of users,

and adherence to all applicable data protection laws (Prewave, 2018b). Further, the company's data protection approach includes a commitment not to grant full exclusivity on generated social unrest event data to any single party, unless the data is used to minimise the risk of suppression of unrest events, or to protect the violation of human rights (Prewave, 2018b).

Under Responsible Data Science, Prewave has access to an Ethics Committee, which provides advice on ethical issues related to the research and work that is carried out in the company. In addition to the Ethics Committee, Prewave engages a variety of stakeholders in its operations:

'through dialogue, posts, case studies [...] that would highlight parts of Prewave development'. (Interviewee 2)

This includes:

'meeting with external stakeholders to ask for their opinions, and to find out about the risks and develop ways to tackle them'. (Interviewee 2)

Why Prewave actively engages in dialogues with stakeholders



Figure 3: Role of Stakeholder Engagement in Prewave (Source: Prewave)

From the discussion above, it can be learnt that although the use of SIS in Prewave poses some ethical concerns, there are remedial actions that have been put in place to address the issues raised in this case study. Similar companies that use SIS for predictive intelligence could learn from the remedial measures that are taken by Prewave and apply them in their business.

6 Conclusion

The Prewave case study has highlighted the use of Smart Information Systems (SIS) in predictive risk intelligence in domains such as insurance, supply chain management and sustainability, in addition to medicine and health science where it has predominantly been applied. In addition to the benefits of using SIS to predict risk intelligence used to inform some decision-making processes for better outcomes in industry or communities, the case study also highlighted some related ethical issues. The issues identified from the interviews in section 5 are comparable to those discussed in the literature in Section 3 and shows that the use of SIS in predictive risk intelligence poses similar ethical issues regardless of the sector in which the technology is used. Therefore, the main ethical issues that have emerged from the case study include protection of the data being used in predicting risk, data privacy of the data subjects and consent from those whose data has been collected from data providers such as social media sites. Also, there are issues relating to the transparency and accountability of processes used in predictive intelligence. Further, the interviews highlighted the possibility of bias in using the SIS for making predictions for specific target clients and therefore formulating algorithms that will service those clients. The last ethical issue was related to trust and accuracy of the predictions of the SIS.

Prewave recognises the possible ethical concerns that relate to the use of SIS in their operations and therefore have put some remedial measures in place to address these issues. For instance, there is an ethical code of conduct together with the active engagement of stakeholders in discussing some of the activities that the company is carrying out.

6.1 Limitations

While a case can be made for the ethical issues identified in this report, it is arguable that the most impressive capabilities of the SIS and therefore the ethical issues related to its use in predictive risk intelligence have not yet been widely explored. Considering that Prewave is a start-up and the technology is still being developed and going through its growth stage, more could emerge over time regarding the ethical implications of the technology. The issues identified in this study are a starting point and only reveal that there are ethical implications for companies using similar SIS to consider. The size of the company and its stage in the development cycle could not give a broader picture because like other technologies, the full ethical effect of SIS use in predictive risk intelligence in SCM, insurance and sustainability will not be realised until waves of complementary innovations are developed and implemented.

6.2 Contribution

There is extensive research on predictive intelligence in medical sciences, but there is a need to develop knowledge in other fields. The case study on Prewave has offered a significant contribution to the discourse on the implementation of SIS, and also around the ethics of AI by highlighting some of the ethical issues that result from the many uses of SIS. Therefore,

the case study has offered a new perception on the use of SIS and its ethical implications in predictive risk intelligence.

6.3 Implications of the Case Study

The case study has implications for theory since it presents original insights from a company that uses SIS in predictive intelligence in SCM, insurance and sustainability. The report has practical implications for the implementation of SIS in industry, particularly for start-ups such as Prewave. Ethics should be a central consideration for companies and individuals developing SIS, in order to create meaningful positive change for society. The ethical issues resulting from predictive risk intelligence in the areas in which the company operates need to be identified and discussed so that they can be addressed. In so doing, companies including start-ups, which are developing similar SIS could use the case study to reflect on their practices and the ethical implications towards society in the future. For instance, the case study has practical implications relating to responsible and inclusive delivery of warnings for events. It has never been more imperative to have an open discussion about the proliferation of technology and how it will affect privacy rights and data security on both personal and national levels. This case study supports such a discussion by showcasing how it is also imperative for researchers, and innovators to take heed of the ethical issues and continue pondering on remedial actions.

6.4 Further research

While the Prewave case study provides a preview of the ethical issues with predictive risk intelligence, there is a need to get an understanding of the larger picture of the issues that are significant when it comes to using SIS in predictive risk intelligence. This should not stop at risk, but also address other aspects of society such as societal welfare. Further research is required to uncover additional ethical issues that relate to this emergent field, with a particular interest in evaluating and identifying the best ways of addressing the ethical issues. Thus, the research would benefit from additional case studies from bigger and leading companies in the sector. It would also be interesting to evaluate the differences in how ethical issues are recognised and addressed between smaller and well-established bigger companies to ascertain mutual learning mechanisms within the sector.

7 References

- Baecke, P., Bocca, L., 2017. The Value of Vehicle Telematics Data in Insurance Risk Selection Processes. *Decis Support Syst* 98, 69–79. <https://doi.org/10.1016/j.dss.2017.04.009>
- Barocas, S., Selbst, A.D., 2016. Big Data's Disparate Impact. *SSRN Electron. J.* <https://doi.org/10.2139/ssrn.2477899>
- Bates, D.W., Saria, S., Ohno-Machado, L., Shah, A., Escobar, G., 2014. Big Data In Health Care: Using Analytics To Identify And Manage High-Risk And High-Cost Patients. *Health Aff. (Millwood)* 33, 1123–1131. <https://doi.org/10.1377/hlthaff.2014.0041>

- Bendoly, E., 2016. Fit, Bias, and Enacted Sensemaking in Data Visualization: Frameworks for Continuous Development in Operations and Supply Chain Management Analytics. *J. Bus. Logist.* 37, 6–17. <https://doi.org/10.1111/jbl.12113>
- Bentley, P.J., Brundage, M., Häggström, O., Metzinger, T., European Parliament, European Parliamentary Research Service, Scientific Foresight Unit, 2018. Should we fear artificial intelligence?: in-depth analysis.
- Brynjolfsson, E., Rock, D., Syverson, C., 2017. Artificial Intelligence and the Modern Productivity Paradox: A Clash of Expectations and Statistics (No. w24001). National Bureau of Economic Research, Cambridge, MA. <https://doi.org/10.3386/w24001>
- Chopra, S., Sodhi, M.S., 2014. Reducing the risk of supply chain disruptions. *MIT Sloan Manag. Rev.* 55, 73–80.
- Cohen, I.G., Amarasingham, R., Shah, A., Xie, B., Lo, B., 2014. The Legal And Ethical Concerns That Arise From Using Complex Predictive Analytics In Health Care. *Health Aff. (Millwood)* 33, 1139–1147. <https://doi.org/10.1377/hlthaff.2014.0048>
- Coyne, S., Madiraju, P., Coelho, J., 2017. Forecasting Stock Prices Using Social Media Analysis, in: 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech). Presented at the 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), pp. 1031–1038. <https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.169>
- Crawford, K., Calo, R., 2016. There is a blind spot in AI research. *Nature* 538, 311–313. <https://doi.org/10.1038/538311a>
- Fischer, T., Krauss, C., 2018. Deep learning with long short-term memory networks for financial market predictions. *Eur. J. Oper. Res.* 270, 654–669. <https://doi.org/10.1016/j.ejor.2017.11.054>
- Geng, R., Bose, I., Chen, X., 2015. Prediction of financial distress: An empirical study of listed Chinese companies using data mining. *Eur. J. Oper. Res.* 241, 236–247. <https://doi.org/10.1016/j.ejor.2014.08.016>
- Gupta, A., 2018. The Evolution of Fraud: Ethical Implications in The Age Of Large-Scale Data Breaches And Widespread Artificial Intelligence Solutions Deployment 7.
- Hacker, P., 2018. Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law (SSRN Scholarly Paper No. ID 3164973). Social Science Research Network, Rochester, NY.
- Hall, W., Pesenti, J., 2017. Growing the Artificial Intelligence Industry in the UK.
- Hamet, P., Tremblay, J., 2017. Artificial intelligence in medicine. *Metab. - Clin. Exp.* 69, S36–S40. <https://doi.org/10.1016/j.metabol.2017.01.011>

- Hazen, B.T., Skipper, J.B., Boone, C.A., 2016. Big data and predictive analytics for supply chain sustainability: A theory-driven research agenda. *Comput. Ind. Eng.* 101, 592–598.
- Horvitz, E., 2017. AI, people, and society. *Science* 357, 7–7.
<https://doi.org/10.1126/science.aao2466>
- Horvitz, E., Mulligan, D., 2015. Data, privacy, and the greater good. *Science* 349, 253–255.
- Isaak, J., Hanna, M.J., 2018. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer* 51, 56–59. <https://doi.org/10.1109/MC.2018.3191268>
- ITU, 2018. Challenges and opportunities of Artificial Intelligence for Good [WWW Document]. ITU News. URL <https://news.itu.int/challenges-and-opportunities-of-artificial-intelligence-for-good/> (accessed 12.14.18).
- Jeble, S., Dubey, R., Childe, S.J., Papadopoulos, T., Roubaud, D., Prakash, A., 2018. Impact of big data and predictive analytics capability on supply chain sustainability. *Int. J. Logist. Manag.* 29, 513–538. <https://doi.org/10.1108/IJLM-05-2017-0134>
- Jordan, M.I., Mitchell, T.M., 2015. Machine learning: Trends, perspectives, and prospects. *Science* 349, 255–260. <https://doi.org/10.1126/science.aaa8415>
- Kant, G., Sangwan, K.S., 2015. Predictive Modeling for Power Consumption in Machining Using Artificial Intelligence Techniques. *Procedia CIRP* 26, 403–407.
<https://doi.org/10.1016/j.procir.2014.07.072>
- Katwala, A., 2018. How to make algorithms fair when you don't know what they're doing. *Wired UK*.
- Keeso, A., 2015. Big Data and Environmental Sustainability: A Conversation Starter (in brief). *Medium*.
- Louzada, F., Ara, A., Fernandes, G.B., 2016. Classification methods applied to credit scoring: Systematic review and overall comparison. *Surv. Oper. Res. Manag. Sci.* 21, 117–134.
<https://doi.org/10.1016/j.sorms.2016.10.001>
- Mani, V., Delgado, C., Hazen, B.T., Patel, P., 2017. Mitigating Supply Chain Risk via Sustainability Using Big Data Analytics: Evidence from the Manufacturing Supply Chain. *Sustainability* 9, 608. <https://doi.org/10.3390/su9040608>
- Meira, W., Jr., 2017. Fairness, Accountability, and Transparency While Mining Data from the Web and Social Networks, in: *Proceedings of the 23rd Brazilian Symposium on Multimedia and the Web, WebMedia '17*. ACM, New York, NY, USA, pp. 17–17.
<https://doi.org/10.1145/3126858.3133314>
- Petersen, C., 2018. Through Patients' Eyes: Regulation, Technology, Privacy, and the Future. *Yearb. Med. Inform.* 27, 010–015. <https://doi.org/10.1055/s-0038-1641193>
- Prewave, 2018a. Introducing Prewave.
- Prewave, 2018b. Prewave | Artificial Intelligence Meets Risk Intelligence [WWW Document]. Prewave Artif. Intell. Meets Risk Intell. URL <https://www.prewave.ai/insurance> (accessed 11.19.18).
- Prewave, 2017. Prewave Case Study: Seaport Closures.

- Singh, A., Shukla, N., Mishra, N., 2018. Social media data analytics to improve supply chain management in food industries. *Transp. Res. Part E Logist. Transp. Rev.* 114, 398–415. <https://doi.org/10.1016/j.tre.2017.05.008>
- Terzi, D.S., Terzi, R., Sagioglu, S., 2015. A survey on security and privacy issues in big data, in: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). Presented at the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 202–207. <https://doi.org/10.1109/ICITST.2015.7412089>
- Torous, J., Larsen, M.E., Depp, C., Cosco, T.D., Barnett, I., Nock, M.K., Firth, J., 2018. Smartphones, Sensors, and Machine Learning to Advance Real-Time Prediction and Interventions for Suicide Prevention: a Review of Current Progress and Next Steps. *Curr. Psychiatry Rep.* 20. <https://doi.org/10.1007/s11920-018-0914-y>
- TU Wien, 2018. Vienna-based AI startup Prewave secures seed investment from IST Cube and Pioneers Ventures – Innovation Incubation Center [WWW Document]. URL <https://i2c.ec.tuwien.ac.at/vienna-based-ai-startup-prewave-secures-seed-investment-from-ist-cube-and-pioneers-ventures/> (accessed 11.19.18).
- van der Aalst, W.M.P., Bichler, M., Heinzl, A., 2017. Responsible Data Science. *Bus. Inf. Syst. Eng.* 59, 311–313. <https://doi.org/10.1007/s12599-017-0487-z>
- Wachter, S., Mittelstadt, B., Floridi, L., 2017a. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *Int. Data Priv. Law* 7, 76–99. <https://doi.org/10.1093/idpl/ix005>
- Wachter, S., Mittelstadt, B., Floridi, L., 2017b. Transparent, explainable, and accountable AI for robotics. *Sci. Robot.* 2, eaan6080. <https://doi.org/10.1126/scirobotics.aan6080>
- Waller, M.A., Fawcett, S.E., 2013. Data Science, Predictive Analytics, and Big Data: A Revolution That Will Transform Supply Chain Design and Management. *J. Bus. Logist.* 34, 77–84. <https://doi.org/10.1111/jbl.12010>
- Wang, G., Gunasekaran, A., Ngai, E.W.T., Papadopoulos, T., 2016. Big data analytics in logistics and supply chain management: Certain investigations for research and applications. *Int. J. Prod. Econ.* 176, 98–110.
- Williams, A.M., Liu, Y., Regner, K.R., Jotterand, F., Liu, P., Liang, M., 2018. Artificial intelligence, physiological genomics, and precision medicine. *Physiol. Genomics* 50, 237–243. <https://doi.org/10.1152/physiolgenomics.00119.2017>
- Xia, Y., Liu, Y., Chen, Z., 2013. Support Vector Regression for prediction of stock trend, in: 2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering. Presented at the 2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering, pp. 123–126. <https://doi.org/10.1109/ICIII.2013.6703098>