Abstract: 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 the literature are reviewed. The empirical case study describes one of the largest distribution system operators (DSOs) in the Netherlands. The aim of this case study is to identify which ethical issues arise from the use of SIS in smart grids, the current efforts of the organisation to address them, and whether practitioners are facing additional issues not addressed in current literature. The literature review highlights 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 revolved 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 were raised in the interviews which are not discussed in the literature. The paper hence highlights the ability of case studies to identify ethical issues not covered (or covered to an inadequate degree) in the academic literature which are facing practitioners in the energy sector.

Keywords: Smart Grids, Ethics, Big Data
Introduction

“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, European 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 Things (IoT) sensors, the increased digitalisation of social life due to robotics and blockchain, 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: invest in upgrading energy infrastructure networks; or 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 in-

---

1 “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

2 “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.
vestments. 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 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 (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. Section 3 will analyse a Dutch DSO 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 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.

The Use of SIS in Smart Grids

The use of SIS 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 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 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).
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.

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
• 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, Luxemburg, 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.
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 tariffs. DSOs are responsible for energy distribution infrastructure (mainly electricity and gas piles, 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.
Not only is the relationship between companies within the energy supply chain 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 prosumer\(^4\). 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

\(^4\) Prosumer: “A prosumer is a person who consumes and produces a product. It is derived from “prosumption”, a dot-com erabusiness 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
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.

**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.

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.

**Health and Safety: Does the smart grid make us unhealthy?**

ORBIT Journal DOI: [https://doi.org/10.29297/orbit.v2i2.108](https://doi.org/10.29297/orbit.v2i2.108)
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).

**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 custom-
ers’ 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 savings\(^5\). 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.

**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. Cyber-attacks 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).

\(^5\) 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

ORBIT Journal DOI: [https://doi.org/10.29297/orbit.v2i2.108](https://doi.org/10.29297/orbit.v2i2.108)
Affordability and energy equity⁶: A new criteria to set society apart

One of the key drivers for the smartification⁷ 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

---

⁶ 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_WEB.pdf)

⁷ smartification (noun): The process of transforming negative behavior into a smart personality.[from the root word smart] (Source: http://nws.merriam-webster.com/pendictionary/newword_display_alpha.php?letter=S&size=20)
the ever-expanding list of electronic gadgets and (soon) electric vehicles available to the more affluent members of society (McCaulay, 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).

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, 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.

The Case of a Large Dutch Distribution System Operator using SIS in Smart Grids

This section will focus on a specific Dutch energy company. The company is a large Dutch 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 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.

Description of Company

The company 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 and it is based in the middle of the Netherlands. It is one of the largest DSOs and part of an energy provider group. There are seven DSOs in the Netherlands, among which three large DSO’s each servicing a different geographical area. The company 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 holding company to ensure that it provides a level ground for all utilities relying on its distribution network.

According to its website, the company 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.” 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 holding company 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.

The company 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 innova-
tion 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.

The company 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. The holding company has also created a living lab, a mid-voltage network 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).

Joint interviews were conducted with members of the Data Protection team within the company. While Data Protection Officers (DPOs) are formally an independent role, the DPOs interviewed reside within the Customer Data domain (departments smartmetering and customer markets). 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 custom-
ers. 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, the company has been proactive in coordinating its 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.

**Description of SIS technologies used in the company**

The company does not yet 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 for smart grid purposes. 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 the company’s customer base, they remain mostly unused for smart grid purposes (see more on this in section 3.3 below) primarily due to lack of clarity in the implementation of privacy laws in combination with energy laws. Despite these tensions, different types of data can legitimately be collected via smart meters:

a) Consumption data collected in 15-minute intervals (electricity) and 60-minute intervals (gas) currently stored within the smart meters.

b) Power quality voltage data are not hard related to energy consumption behaviour of individual households. Power quality data relate to voltage spikes and dips and are made available through smart meters because of their less privacy sensitive character (voltage spikes and dips have no hard relation to specific energy usage of households). In addition, such data cannot be requested by third parties.

c) Power quality data (current related) is directly related to energy consumption behaviours. This type of data is treated the same as consumption data. Power quality current data is not lightly made available via the smart meters and also cannot be requested by third parties.

d) Pinging the meter, to ensure control of and access to the meter by the company.

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 taxpayers money. The company aspires to use smart meter data for various purposes such as:

ORBIT Journal DOI: [https://doi.org/10.29297/orbit.v2i2.108](https://doi.org/10.29297/orbit.v2i2.108)
• 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 from the energy law 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 possible 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 possible 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 the company’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.

The effectiveness of using SIS for the company
Both interviewees agreed that the use of AI for the company 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, company has come together with the other DSOs serving the Netherlands to develop a code of conduct for the branch 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.

**The Company: Ethical issues from SIS Technology**

This section aims to identify which ethical issues have arisen for the company, 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 the company, 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.

**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 the company’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 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.

**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 the company representatives, 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 may disrupt the function of the grid, but also the 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 the company, 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 Act that will affect the management of critical infrastructures and related equipment as well as consumer products (EC, 2017).

Other issues

Data stewardship and market dynamics: the company 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, the company recognises that balancing energy provision be-
tween 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 pri-
marily to issues of distributive justice. Transparency in energy distribution and the use of
“explainable AI”9 that can provide evidence of energy distribution choices and inform
social debates is likely to become pertinent in the future and is fundamental for establish-
ing the social capital and procedural justice that can springboard technology acceptance.

**Mechanisms for addressing ethical issues**

The company recognises that engagement of the public has been relatively low and local-
ised, 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 pro-
gramme to engage customers and relevant NGOs more substantively.

The company 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 devel-
opment 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. The company is also keen to develop a scheme to engage the public
in dialogue to address their concerns.

**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 company 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 pri-
vacy. Privacy directly relates to household energy consumption data currently collected
and stored in smart meters. Privacy issues are seriously debated and are affecting the in-
stallation of smart meters in households in the Netherlands to the desired 80% level. Pri-
vacy concerns are thus presently a key barrier for the rollout of smart meters and their

---

9https://en.wikipedia.org/wiki/Explainable_Artificial_Intelligence
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 the 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 living lab 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; 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.

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.

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.

Acknowledgements
This SHERPA project has received funding from the European Union’s Horizon 2020 Framework Programme for Research and Innovation under the Specific Grant Agreement No. 786641. The author acknowledge the contribution of the consortium to the development and design of the case study approach. They are grateful to UCLan Cyprus for their contribution to quality assurance of the case study.

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_a89a14c136f0aec5b771404bc5b191e9. [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 [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.rrij.com/open-access/a-review-of-power-qualityproblems-and-solutions-in-electrical-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 CIIs: Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII) Available at: The cost of incidents affecting CIIs.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].