Purpose and fuction creep by design: Transforming the face of surveillance through the Internet of Things

Wisman, T.H.A.

published in
European Journal of Law and Technology
2013

document version
Publisher's PDF, also known as Version of record

Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things

T.H.A. Wisman [1]

Cite as Wisman, T.H.A., "Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things", European Journal of Law and Technology, Vol. 4, No. 2, 2013

Since 2006 the European Commission expresses the ambition to transform our current Internet from a network of computers to a network of things and to increasingly merge the physical and the digital world. [2] This new Internet will be an Internet of Things, a network that autonomously sets flows of data in motion without direct human involvement. Another thing that the IoT allows is the control over devices from a distance. Neelie Kroes said that the Internet of Things "is surrounded by a value system: as it comes so close to the heart of everyday life, social relations and daily services, it needs a broad societal consensus to fulfill its potential." [3]. The processing of data regarding these highly intimate aspects of citizens their lives could have an enormous impact on their privacy. The potential of the IoT to fuel a surveillance society through purpose- and function creep is a subject that has a less prominent place in the mainstream discourse of the European Commission.

1. Introduction

As the economy of Europe is crumbling, politicians are desperate to grab on to anything that might save society. Companies are more than willing to provide a panacea for all the problems that are perceived, a vision to be trusted and to be invested in: society should be safer, cleaner, more comfortable, more efficient and more secure. To realize efficiency in society, up-to-date information about vital processes is indispensable. The more detailed this information is and the more parties have access to it, the more accurate decisions can be taken. So what would be more attractive than a society that provides the means of collecting data on an unprecedented scale? Although the skeptic, or realist for that matter, might deem this a bit optimistic, the fact is that the EU actively collaborates with industry to get this vision airborne. There is no common denominator for this utopian vision in the mainstream, but the EU uses the term the *Internet of Things* (hereafter the IoT) to formulate and build a special part of their ICT-policy. The central idea is to weave ICT into the fabric of everyday things, connect them to the Internet and thus create an intelligent network that, according to EU-reports, "will stimulate economic growth, improve individuals' well-being and address some of today's societal problems". [4] According to expectations expressed by the European Commission 50 billion things will be online by 2020, creating a vast web of things that can be accessed from anywhere. [5] According to the Head of Unit Internet of Things from the Commission, Gérald Santucci, the IoT even has the potential of connecting the 100,000 billion things that are deemed to exist on earth. [6]

A very broad definition of the IoT is given by CASAGRAS (Coordination And Support Action for Global RFID-related Activities and Standardisation) as "a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability." [7] This definition is in line with the approach taken in EU documents on the IoT which entails more than TCP/IP communications, in other words the underlying network does not have to be Internet. Objects in the IoT cannot only be accessed, but also "read, recognised, addressed, located and/or controlled remotely" [8] through the Internet or other network infrastructures. Another key quality of the IoT is that the *things* autonomously collect and exchange data. [9]

The drawback of the IoT vision is that it only takes a few tweaks to turn this tailored-service-society [10] into an unprecedented surveillance-society. On top of that IoT-devices can become mandatory by law. The technology that is used by customers to access services can be used to monitor and interfere with the activities of the customer. The use of technology to perform a function it was not originally intended for constitutes *function creep*. The data generated in the course of using these services can be used to personalize the service, but also to profile the customer. The use of data for a different goal than it was collected for results in *purpose creep*. [11] The purpose of the IoT to realize a smooth functioning information society may (also) turn into the perfect tool to realize a surveillance society. On top of that the EU invests in security projects, some of which interlock with the IoT.

This paper addresses the question whether the policy of the EU with regard to the IoT does not amount to a purpose- and function creep by design that conflicts with the right to privacy as protected by Article 8 ECHR? The first part of this paper explains how EU funding contributes to realizing the IoT vision and uses examples to reveal how this relates to surveillance activities. The second part is used to explain how IoT-devices enable authorities to exercise control from a distance and to construct my hypothesis that EU policy on IoT guides a process aimed at the capturing of people their everyday behavior. IoT-devices will autonomously set flows of data in motion which are transmitted over publicly available electronic communication networks which results in a large amount of data that could fuel the future surveillance assemblage of Europe. Furthermore I argue why the IoT will have a transformative effect on the face of surveillance.

2. EU Policy on the Internet of Things

The IoT was on the Commission's radar already before the Action Plan on the IoT was released. In a roadmap on Radio Frequency Identification (RFID) from the Commission in 2006 the IoT is already mentioned [12], as well as in a speech of Viviane Reding, the Commissioner Information Society and Media at that time. [13] In 2007 the Commission published a Communication on RFID in Europe, in which the IoT is repeatedly mentioned and guidelines for IoT policy are formulated. [14] The term *Internet of Things* is even older and was introduced in 1999 by Kevin Ashton in a presentation for Procter & Gamble:

"If we had computers that knew everything that there was to know about things - using data they gathered without any help from us - we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best." [15]

I again emphasize this essential characteristic of the IoT: data flows are autonomously set in motion, without direct human involvement. Another description Ashton gave of the IoT was "a standardized way for computers to understand the real world". Ashton was asked by P&G to optimize the management of the supply-chain of Max Finity lipsticks. RFID-tags, a case with a chip containing a unique number and an antenna (nowadays often to be found on more expensive, easy to steal products that you buy, e.g. usb sticks), were put on the lipsticks. In the shelves a reader, a device that generates electromagnetic waves at a regular interval, activated the present RFID-tags and the unique numbers were transmitted to the P&G computer database thus enabling more accurate supply-chain management from anywhere in the world. [16] When the product was bought the RFID-tag would be removed. But what kind of opportunities would arise if you would leave the tag intact? A Commission Recommendation of 2009 discusses the use of tags in (household) applications and mentions the option for the consumer to decide upon whether the tag remains active. This approach is also known as opt-in. In 2008 EPCglobal[17] already objected to opt-in and proposed opt-out, an approach in which the tag is left intact by default unless the consumer decides otherwise. It seems that the Commission endorses the vision that products consumers buy, could contain a tag that is used to communicate to household-applications, e.g. RFID in clothing communicating with the washing machine about the appropriate program to run. [18] The idea of voluntary IoT participation was also confirmed by the European Parliament. [19] In later EU documents the implementation of the IoT mentions 18 domains in society ranging from automotive to medicine. [20]

2.1 Funding the Internet of Things

One way the EU actively contributes to the emergence of the IoT is funding. Some initiatives are easy to categorize as "IoT-funding", others are less directly linked, but inevitably contribute to the IoT and arguably the surveillance apparatus in the EU. One of the main programs for funding is the Seventh Framework Programme (hereafter FP7). In Viviane Reding's 2006 speech about the European RFID policy, she referred to FP7 and how this program is supposed to foster collaborative research on RFID. FP7 fits the ambition of the EU to become "the most dynamic competitive knowledge-based economy in the world" [21]. The budget is €53.2 billion for 2007-2013 (€7.6 billion a year). Commissioner Máire Geoghegan-Quinn also recently announced a €80 billion package for FP8 2014-2020 (approximately €11.4 billion a year). [22] This is a significant increase compared to the FP6 budget of approximately €3.6 billion a year. The ambitions of FP7 are broad. This seven-year program has two main objectives:

- "to strengthen the scientific and technological base of European industry;
- to encourage its international competitiveness, while promoting research that supports EU policies." [23]

The ten key thematic areas of FP7 coincide almost completely with the application domains of the IoT as mentioned in the report of the Cluster of European Research Projects: [24]

SEVENTH FRAMEWORK PROGRAMME	CLUSTER OF EUROPEAN RESEARCH PROJECTS IOT
Health	Medical Technology, Healthcare + Pharmaceutical
Food, agriculture and fisheries, and biotechnology	Food traceability + Agriculture and Breeding
Information and communication technologies	Telecommunication
Nanosciences, nanotechnologies, materials and new production technologies	Manufacturing, Product Lifecycle Management
Energy	Oil and Gas
Environment (including climate change)	Environment Monitoring
Transport (including aeronautics)	People and Goods Transportation + Automotive + Retail, Logistics, Supply Chain Management + Aerospace and aviation
Socio-economic sciences and the humanities [25]	Independent Living + Recycling + Insurance
Space	Aerospace and aviation
Security	Safety, Security and Privacy

These categories are not directly related to surveillance, but can have an impact on the way surveillance is embedded in society. Transport, for example, entails clean and safe vehicles. [26] In an International Telecommunication Union report on the IoT, speculations are already made about RFID-systems in cars (mandatory by law) to measure tire-pressure. [27] Neelie Kroes, the Commissioner for Digital Agenda, announced in 2011 that cars should be equipped with a system that independently dials emergency services whenever the car crashes. [28] The eCall-system locates the car through GPS [29] and currently there is a pilot project funded by €5 million from the Commission. [30] Although cloaked in terms of benevolence, this plan implies the mandatory installation of military localization equipment in every new car in the EU starting 2015. It does not take a lot of imagination to visualize the police using this system when a car is stolen, or when a policeman is genuinely interested whether his wife is really spending the weekend at her mom's place. [31]

This is just one example, but there are more fields in which the general FP7-funding may contribute to the IoT-vision. The similarity between the key thematic areas of FP7 and IoT are striking and obvious.

2.2 Direct funding for the IoT

Projects supporting the IoT-vision receive money directly from FP7 through the ICT Work Programme, which pertains to the key thematic area of Information and Communication Technologies and receives a total of € 9.1 billion, the biggest share of all research themes in the Cooperation Programme. [32] In the ICT Work Programme 2013 the IoT is explicitly mentioned in four policy agendas - healthy ageing, smart cities, pervasive and trusted network and service infrastructures- two of which will be treated in the light of surveillance.

First of all, the IoT will play a role in healthy ageing. Under the header European Innovation Partnership (EIP) on Active and Healthy Ageing' [33] the 'Personalised health, active aging and independent living' objective is set, which is supposed to increase the healthy lifespan of EU citizens by two years. An example of a project is ICARDEA (Commission Funding €2.539.833 million) [34]: An Intelligent Platform for Personalized Remote Monitoring of the Cardiac Patients With Electronic Implant Devices. Although an initiative like this clearly serves the people under surveillance, through purpose creep this data, or even worse through function creep the devices, might be used for other goals. SWAMI, an EU report on 'Ambient Intelligence' - a term that is considered interchangeable with IoT -states that IoT devices "such as implants or technologies that monitor our physiological condition and behaviour could well make our society more secure, particularly if they enable law enforcement authorities and intelligence agencies to take preventive measures." [35] Although this harsh claim is slightly nuanced by the author, it does show a form of function creep of which the thought alone would be detrimental to the health of any person wearing such a device. It seems rather contradictive and counterproductive to express this thought in a report which recognizes that trust is a possible obstacle for realizing the IoT, as well as a necessary feature of life in contemporary society. [36]

Second, the IoT is mentioned in the context of smart cities. One of the key issues in this area is clean and efficient energy. This also comes back in the sixth challenge that deals with the low carbon economy. One of the means to realize this goal is the transformation of our current electricity grid into a smart grid. In a nutshell, the smart grid will enable a better coordination of the demand and supply side of the electricity grid and this will reduce the amount of peak demands and thus save energy. Around € 5.5 billion is invested in smart grid [37] projects, of which €300 million comes from EU budget. [38] According to Annex 1 in the Directive 2009/72/EC concerning common rules for the internal market in electricity [39] at least 80% of the consumers shall be equipped with smart meters by 2020, if the roll-out is assessed positively. Smart meters register the electricity consumption at a regular interval, fifteen minutes is the consensus representatives of Member States and the Commission reached. [40] These smart meters enable the metering operator to read these registrations from a distance whenever he wants. In 2004 there were already meters deployed in Finland that uploaded electricity data to the operator in real-time. [41] This data exposes certain behavior - the time someone starts using electricity, stops using electricity, the changes in the usage pattern - they all amount to the detail of the picture that can be drawn about the life of the customer, it can even create insight into someone's religion. [42] Another new quality of the smart meter is that it allows the smart meter operator to shut the supply of electricity down without entering the home. [43] In one of the EU reports on the IoT it can be read that smart meters[44] in conjunction with modern home entertainment systems could be combined with "other sensors and actors within a building, thus forming a fully interconnected, smart environment". [45] Smart meter communication to devices over the Internet will create location- and traffic data, besides sensitive data might be stored on smart meters themselves available for the operator to request . [46] This example shows how the unbounded character of cyberspace combined with intelligence embedded in objects bypasses the traditional boundaries of the home and quietly penetrates the private sphere of citizens.

Although most challenges in the ICT Work Programme are not explicitly brought under the scope of the IoT, they are all directly or indirectly related: "Cognitive systems and robotics", "alternative paths to components and systems", "technologies for digital content and languages",

"ICT for the enterprise and manufacturing", and "ICT for learning and access to cultural resources". For instance, convergence of the embedded and Internet worlds, of nanoelectronics, nano-materials and ICT is mentioned in the challenge "Alternative Paths to Components and Systems" and is not directly linked with the IoT, but corresponds with the central idea behind the IoT to merge online and offline environments. [47] Because it is not possible to draw a straight line between IoT and non-IoT projects, it is impossible to give an exact number of funding that is invested in the IoT by the EU. Approximately direct funding can be estimated as €70 million [48], while indirect funding can go into hundreds of millions [49] or maybe even more.

2.3 Interlocking security projects

Besides IoT-projects there are also specific security projects that do not directly relate to the IoT, but these projects indicate how IoT-developments interlock with surveillance-ambitions. In 2004, the Commission put together a Group of Personalities (GoP) that insisted on more public funding for research and technology, through which Europe could become more secure for its citizens. [50] A lot of these personalities were heavily involved in the security and military industry, which gives their advice a tone of "we, the people of the security industry, recommend to you more security!" This did not seem to bother the Commission and in 2004 a Communication [51] almost literally repeated the report of the GoP:

"Political, societal and technological developments have created a fluid security environment where risks and vulnerabilities are more diverse and less visible." [52]

On page 5 of this Communication the Commission welcomes the GoP report, and subscribes to the main recommendations and orientations, and promises to undertake, in collaboration with the stakeholders, necessary actions including the establishment of a European Security Research Programme (ESRP) as part of FP7. In FP7 the Commission reserved € 1.4 billion for security research alone. "Making Europe more secure for its citizens while increasing its industrial competitiveness, is the goal of European Security Research." [53]

For reasons of space, I only give as an example the most remarkable security project within this program, INDECT. According to the current site of the Commission this project aims at improving accuracy of existing video surveillance through the development of algorithms that identify dangerous and criminal behavior in public. [54] The page emphasizes that there is not a plan for a European wide Orwellian surveillance system and that there is no secret information that has not been published, everything can be found on the website. However, they do not mention that when critical reactions started to pop up as a result of the previous website, it was heavily renovated, including the disappearance of the documents concerning all deliverables,. Luckily these pdf's are easily recoverable on the web. [55] They match the originals downloaded from the first INDECT-site, in case the reader questions the authenticity of these files. The original acronym Intelligent Information Sytem Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment, which is missing on the current website [56], can be found on the front page of this pdf. The aim of INDECT's "Work package 4" is to develop technologies to facilitate the building of an Internet based intelligence gathering system, objective 4.1 talks about a relationship mining system through websites and social networks. [57] Imagine the privacy impact if data used in INDECT, or any other surveillance

project crawling the Internet, is fueled by IoT-systems that autonomously set flows of data in motion over the Internet.

3 Transforming the face of surveillance

Smart meters, smart devices, medical implants and other gadgets will set more and more data flows in motion. Surveillance technology will be omnipresent in the future. Now what is the difference between placing a piece of surveillance equipment and someone using a device that records exactly the same information? First of all, the use of surveillance equipment directly exposes the data that is captured to the entity that placed it there. The data that originates from a device that someone uses, it has to be firstly accessed. Second, while for now the use of the device depends on a voluntary choice, it is unsure how voluntary the IoT will be in the future, given the persuasive approach that is taken in many EU reports. [58] Besides, you could argue that most people are not aware of the invasive qualities of certain technology and it is unsure whether they would still be using this technology if they knew. I have no exact figures, but when I talk with informed people, viz. working in the same field, law and ICT, the majority does not know that, e.g. every mobile phone is equipped with a backdoor that allows the police to turn on the microphone or the camera, even if the phone is switched off. [59] This way the police can overhear every conversation you have in the proximity of your phone. This indicates how little my peers know about this reality, let alone the general public. The third difference is that the person under surveillance probably is not aware of the presence of any surveillance equipment. This might make him less careful. Most people surround themselves with surveillance equipment without being aware of it. The more time passes by, the more people will become aware of the invasive character of the technology that surrounds them. Awareness is one thing, but knowing exactly what data is processed in what way by simply interacting with your environment is another story. Los argues that this inability to understand what is happening around us, could have a paralyzing effect on people, as their sense is growing of "being helpless in face of the omnipresent, interconnected and internationalized surveillance". [60] This effect is also defined as the disciplinary effect of scrutiny, the central idea behind the prison-design commonly known as the panopticon. Jeremy Bentham who is regarded as the initial designer of the panopticon referred to it in the following words: 'a new mode of obtaining power of mind over mind, in a quantity hitherto without example.'[61]

Bentham's panopticon is child's play compared to surveillance in a fully functioning IoT. It would for example be in line with the vision of controlling objects through the Internet to implement a function in the eCall-system that could remotely shut a car down. [62] In fact another functionality that the smart meter will be equipped with is the ability to shut down the supply from a distance. [63] The vision of the IoT allows government to go beyond passive surveillance; it creates an infrastructure that enables authorities to take measures from a distance that directly affects the life of the citizen. This means a fundamental shift in the power relation between the citizen and public authorities, which allows the latter to exercise power at a distance. Schermer described this as the shift "from an 'architecture of observation' to an 'architecture of control' which will negatively impact the autonomy of individuals and groups who move through the public domain to a far greater extent than currently possible". [64] The private domain will be equally affected. It seems that the invisible hand of the market is getting company in the form of the invisible hand of surveillance manifested in the constant threat of intangible power that

can be exercised against people when they are not conforming their behavior to the societal norms. This thought interlocks in a way with the reason why Lessig believes that the Internet should not be governed by the market:

"There is no reason to believe that the foundation for liberty in cyberspace will simply emerge…. we have every reason to believe that cyberspace, left to itself, will not fulfill the promise of freedom. Left to itself, cyberspace will become a perfect tool of control." [65]

Without claiming that this rather ambitious surveillance-project is officially pursued by the EU, I will use the remainder of this paper to substantiate my hypothesis that EU policy with regard to the IoT guides a process leading to capturing people their everyday behavior by IoT objects & devices which will autonomously set flows of data in motion transmitted over publicly available electronic communication networks. This large amount of data fuels the future surveillance apparatus within Europe. A final step in realization is removing the 'obstacle' of privacy legislation in combination with the standardizing and mandatory retention of IoT-data.

3.1 Privacy in the IoT

Privacy in the IoT results in a paradoxical policy objective, since one of the key drivers in the IoT is to connect everything and the right to a private life is about protecting an intimate sphere that requires some form of isolation. In its Action Plan on the IoT (2009) the Commission places privacy and data protection under the header of "Lifting the obstacles to the uptake of the Internet of Things". They state that "social acceptance of the IoT is strongly intertwined with respect for privacy and protection of personal data" and that appropriate data protection measures are a prerequisite for trust and acceptance of "these systems". The Commission considers that the uptake of the IoT will affect the way we understand privacy. The argument behind this consideration seems to be that the ongoing development of technology has an effect on our system of values. This argument supports to some extent a self-fulfilling prophecy, since policy and legislation from the EU itself is contributing to the development of technology that they ascribe this quality to. If you follow this logic the EU is indirectly, yet actively, contributing to changing the value of privacy. This somewhat technological deterministic view shimmers through EU reports and insinuates that there is no power to be exercised over the way technology is implemented in society, dislocating the accountability of government for their role in this process. From a legal point of view the argument that the development of technology sets the norm seems strange, it should be the other way around. The emergence of Privacy by Design (PbD) and Privacy Enhancing Technologies (PET), on top of common sense, tells us that engineers are able to build ICT-systems in pretty much any way they like. This displays the falseness of the underlying argument on which this laissez-faire attitude is based.

An episode of the Dutch documentary-series *Backlight* illustrated that the effect that computers have on privacy is really a matter of choice. Ann Berg (a former speculator) tells that on the exchange of Chicago it is possible to buy 22 000 contracts on corn, which is almost 3 million tons (around 55 panamax ships) through a black box system that guarantees the anonymity of the buyer. [66] She continues to explain that before the emergence of the computer it was not possible to make these transactions anonymous, because the people were visible on the floor where they traded. This development seems to indicate that there is a reverse process taking

place with regard to data of high level transactions in the financial world, compared to data about everyday life activities of normal citizens. Every action from switching on your phone when you wake up, to checking in at the train station, entering the office with your personal card, and making a phone call to your mom during lunch, is registered and accessible. However, if you decide sometime during the day you should invest in an amount of grain that, when taken of a specific market, could easily set off a revolution, this information stays below the radar.

It would not be right to accuse all EU politicians of taking a passive stance regarding the privacy-issues of the IoT. There is one informal group that pro-actively looks for "the opportunity, for informal fireplace-like discussions among Ministers on political themes". "It was stressed that the Group gives upcoming presidencies and the Commission the chance to communicate in an open and informal way before concrete proposals and drafts are produced." [67] "The Future Group" that refers to itself as the Informal High Level Advisory Group on the Future of European Home Affairs Policy, largely consisted of several internal ministers and experts. [68] Unfortunately the fireplace-like discussions were clearly aimed at burning privacy down to the ground:

"Every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organizations, and create huge opportunities for more effective and productive public security efforts." [69]

This remarkable quote about the IoT can be found in a proposal published already in 2007. The proposal served the Council of the EU in preparing the Stockholm Program on justice, freedom and security. This phrase is written specificly on the IoT and how it can be used as an instrument of unprecedented surveillance. Unsurprisingly, American intelligence agencies also see the opportunities in this new Internet. The director of the CIA stated that *transformational* is an overused word, but that it applies to the IoT. He was very clear in an interview when he talked about the IoT and stated that: "The resultant chorus of 'connected' devices will be able to be read like a book - and even remote-controlled". [70]

3.2 Data protection or data dispossession?

One of the most popular definitions of informational privacy is the one of Alan. F. Westin: the claim of individuals to determine when, how and to what extent information about them is communicated to others. [71] In practice this right is often balanced against other interests like the rights of others, national security, public order and the economic well-being of a country, also to be found in Article 8(2) ECHR. In the EU the rules for the handling of personal data are laid down in Directive 95/46/EC. Data protection is sometimes used interchangeably with informational privacy. The way data protection today is positioned by the Commission, however, is very different from Westin's definition of informational privacy. To put it bluntly, the creative approach of the Commission to data protection hands over the right to self-determination to the government and let them decide when, how and to what extent information about the individual is communicated to others. [72] The link with the right to respect to private life as put forward in Article 8 ECHR, the original anchorage of the Data Protection Directive [73], gradually moves to the background. The balancing between the rights of the individual to the respect of the private sphere and the public interest seems to be irrelevant as long as the data is gathered under strict

conditions for a legitimate purpose. There is no doubt that in certain circumstances the collection and sharing of data is justified. However, if society is constructed in a way that every act of the individual causes the processing of data that is captured in databases accessible by public authorities, the principle of proportionality is neglected. The steady appeal of the Commission to data protection to safeguard privacy in the IoT displays little concern for the context in which this *fundamental right* [74] should function. This justifies the question whether data protection should not be relabeled *data dispossession*.

Informational privacy is meant to give the individual some safeguards and control over the data processed regarding him or her. The rationale is that processing of data can have implications for personal freedom. This idea was already acknowledged in a society where computers were as big as elephants, and index cards were regarded as modern means of administration. The borderless character of the IoT will increasingly permeate every aspect of life. This does not only infringe upon informational privacy, since this development crosses the borders of the private sphere, registering people their behavior in their own house, therefore directly interfering with the right to respect for private life. [75] This will affect people their behavior and condition the way they perceive their environment and themselves.

There are roughly two arguments for a stronger interpretation of data protection that goes beyond adequate data management and fully acknowledges the limiting effect of the processing of personal data on individual freedom. In the first place it is important that the individual is not scrutinized in everything he or she does, because this will result in a disciplinary effect that was already treated in one of the previous paragraphs. [76] A person is not able to act freely if all or most of his or her actions suffer under the disciplinary effect of scrutiny. The underlying value of this argument is freedom. Second, the unbridled registration and processing of personal data can result in decisions being taken that affect the individual without any understanding how other actors arrive at this decision. [77] The underlying value of this argument is autonomy.

3.3 Fuelling the surveillance engine

Before the digitalization of society, data was either not created, or only stored locally. Through modern ICT, however, data attained a different character. It transformed from *isolated* data used in a single context to *connected* data that serve a multitude of contexts. This transformation allows data to become fuel for a surveillance society that is constructed on the footing of connectivity and interoperability, in EU parlance on the IoT sometimes fused together as *interconnectivity*. This term is used in many EU reports on the IoT to express the desire to standardize data, allowing it to irrigate every aspect of life in a digitalized society. [78] Although it could be argued that processing data this way does not contribute to the integrity of data, since the meaning derived from it is context-dependent, the plea for efficiency is hard to counter. According to the Cluster of European Research Projects on the Internet of Things (CERP-IoT)-report the advancement of technology renders the processing capabilities more accessible and versatile "the opportunity for even tighter interconnectivity is fuelling the desire to make use of these possibilities". [79] This sentence catches a very important characteristic in the attitude of policymakers when it comes to the sharing of data: if it is possible, than why should we not do it? This echoes Hannah Arendt's thought on science. According to her it is not so much about what we want, but more about what we can, that forces people to do the possible, despite the

consequences. [80] The pragmatic approach to the processing of data sharply contrasts with one of the fundamental principles of the Data Protection Directive [81] in Europe, i.e. the purpose specification and limitation principle. This principle requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. [82] It is remarkable that further processing incompatible with the purposes of the original data collection, in other words *purpose creep* seems to be a core value of EU's IoT vision.

The fact that the data in the IoT will be mostly routed over the Internet creates a problem with regard to privacy. Every interaction with a device over the Internet leaves digital traces in the form of traffic- and location data, which are retained in EU countries under the controversial Data Retention Directive 2006/24/EC. [83] Under the Data Retention Directive the data is made "available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law." [84] This way data that is gathered for one goal, providing services to consumers in the IoT, will latently and simultaneously serve another goal as well, namely feeding into the surveillance apparatus of the state. Although this is not a new phenomenon in itself, it already happens with the current data that is transmitted over publicly available electronic communication networks. The amount of data and the level of detail will increase dramatically and will leave less space for citizens to keep information about their lives to themselves. In Article 1 of the Data Retention Directive the aim is set to "harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data". Consideration 13 makes clear that it only relates to "data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated". Later this is confirmed in Article 1 (2). In a footnote of the proposal of the draft framework decision on the Directive it is written that the Presidency proposed to replace "data" by "communication data" in Article 1 to prevent confusion about the kind of data that is meant and "in particular to make it apparent that content data is not included". Clearly, the thought behind this is that this type of data is less personal and this justifies the retention. However, if the Data Retention Directive is applied to IoT-systems that will lead to a continuous increase of the processing of "communication data" it becomes all the more evident that this thought is or soon will be outdated. This can be illustrated by some elaboration on the previous examples from paragraph 1.1.

When people start wearing medical devices that are connected to the Internet the location data of these medical devices do not differ from the data that is acquired through any other tracking device. The traffic data that is produced might even reveal highly personal information regarding ones health. When Jay Radcliffe, a hacker, announced that he found security holes in his own insulin pump, he showed the world that privacy is not the only concern here. [85] He proved to be able to command insulin pumps from a similar type to dispense a fatal dosage of insulin. This might sound like a patients' nightmare, still it should not be disregarded that possibilities like these could be very useful for intelligence agencies to take preventive measures. [86]

The example above is a glance into the future. However, smart meters are already here and show interesting potential for surveillance combined with the Data Retention Directive. Although there is no reference made in the recommendation on the roll-out of smart meters [87] to the Data

Retention Directive, by stating that Directive 2002/58/EC [88] is fully applicable to the processing of personal data by smart meters, "in particular in the use of publicly available electronic communications services for contractual and commercial relations with customers" the communication of the smart meter is explicitly brought under the scope of the Data Retention Directive. In the future smart meters will be able to communicate with smart devices when they are equipped with a so-called Home Area Network (HAN) gateway that enables this communication. [89] This is one way that the IoT can recognize, locate, address and/or control objects remotely through the Internet. [90] Although smart devices are not yet a widespread phenomenon, a recent study from IMS research predicts the global shipment of around 400 million 'smart home energy devices' (including smart appliances) in the next five years. [91] Communication to devices over the Internet will create location- and traffic data and sensitive data might be stored on smart devices themselves. [92] A telephone bill shows you the numbers you dialed, the actual time and the length of your call. It is not hard to imagine an evenly detailed report on the devices that are used in the home. It could be that the utility requires the customer to register his HAN device with the utility, in order to establish a secure connection; in that case the utility knows which *specific* device is used. The registration may also expose when a device of a visitor is plugged in, e.g. electric vehicles that are recharged. When you are home and what you are doing in the privacy of your home is personal and intimate information. Moreover, it is doubtful whether indoors communication, e.g. between a person and his blender, will proof to be a valuable tool in the original aim of the Data Retention Directive, i.e. the fight against (organised) crime and terrorism.

4 Concluding remarks

The question that remains is if the policy of the EU with regard to the IoT amounts to a purpose- and function creep by design that conflicts with the fundamental right to privacy as protected by Article 8 ECHR? An affirmative answer implies an accusation of the responsible bodies of the EU, viz. that they are willingly setting up an infrastructure that aims at an omnipresent surveillance regime. Answering with a simple yes or no is attractive, but the area discussed in this paper is rather grey. Privacy always comes back in the communications from the Commission and the EP as an important issue that should be taken care of. Although the (explicit) intent is missing, the effect - purpose- and function creep by design - can still arise.

The current approach that the Commission takes to privacy seems to be misguided by the idea that privacy can be sufficiently safeguarded through data protection. However, when data leave the exclusive control of the individual, this data might be protected according to the law, but still there will be a breach of privacy. Data protection is fundamentally different from privacy and is not suitable to replace this right that is deemed essential in modern day society. The Commission stimulates the development and implementation of technology through a number of funding programs and through the proposal of directives, but is not actively formulating adequate policy with regard to privacy. This makes a rather unbalanced impression. It is surprising how few hackles are raised when a vision that is based on this corporate incentive, is adopted as public policy and is heavily funded with public money-especially when these corporate interests are realized through the implementation of a structure that has a negative impact on privacy and personal freedom, values that are deemed indispensable in a constitutional democracy. What makes this development even more questionable is the fact that what causes this negative impact,

the registration of personal data and the control from a distance over IoT-devices, is beneficial for industry as well as government.

Digitalizing people their environment in a way that silently increases the digital footprints they leave behind, together with the roll-out of devices that allow control from a distance, creates a vast web of surveillance points in society. This process should not be discarded by politicians under the flag of technological determinism, it is a political choice and therefore they should take their responsibility. The process that guides the IoT is largely devoid of democratic legitimacy. It is cooperation between government and industry that is taking place outside of the public arena which, inevitably, will have a great impact on citizenship in our society. The principles that guide this process are corporate in nature and do not have anything to do with democratic values. By the time the individual experiences the impact of this grotesque project, he or she might be tied down by a web of digital strings, each by itself not a great threat to personal freedom, but the accumulation of which is strong enough to keep him bound tight to the digital ground. [93]

---

[1] Tijmen Wisman is a Ph. D. student at the VU University Amsterdam, Faculty of Law.

[2] 'Internet of Things - An action plan for Europe', p. 2 (Brussels: Communication from the Commission to the

European Parliament, the Council, the European Economic and Social Committee and the Committee of theRegions, 2009) http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf, last seen December 1th, 2011.

[3] The 2nd Annual Conference Internet of Things Europe 2010 Conference Report, A Roadmap for Europe, Held on 1st and 2nd of June 2010, Brussels, p. 2.

[4] 'Internet of Things - An action plan for Europe', p. 4 (Brussels: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of theRegions, 2009) http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf, last seen December 1th, 2011.

[5] See http://www.wired.com/beyond_the_beyond/2011/02/spime-watch-the-internet-of-things-a-window-to-our-future/ , last seen November 27th, 2012.

[6] Gérald Santucci is Head of Unit Internet of Things and Future Internet Enterprise Systems, European Commission, see http://www.digitalarti.com/files/Digitalarti-5_UK-site-internet-MD.pdf , last seen November 27th, 2012.

[7] Casagras Final report page 10. See http://bit.ly/XFaEXX, last seen January 24th, 2013.

[8] European Parliament resolution of 15 June 2010 on the Internet of Things, paragraph E.

[9] Cluster of European Research Projects on the Internet of Things, *Visions and Challenges for Realising the Internet of Things*, European Union, March 2010, p. 43.

[10] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, Brussels 15.3.2007, COM (2007) 96 final, p. 3.

[11] The credits for this term go to my supervisor, A.R. Lodder, who challenged my use of the term 'function creep' in a conversation we had. He proposed the term 'purpose creep'. Later we discovered that the term is also used by Nicola Jentzsch in his book *Financial privacy: an international comparison of credit reporting systems*, 2nd ed., Berlin: Springer, 2007, p. 39. According to him it 'describes the tendency to use information for purposes that are unrelated to the original one for which the data was originally collected.'

[12] See http://bit.ly/TuwSis, last seen November 29th, 2012.

[13] See http://europa.eu/rapid/press-release_SPEECH-06-597_en.htm?locale=fr , last seen November 27th, 2012.

[14] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, Brussels 15.3.2007, COM (2007) 96 final.

[15] See, Ashton, K. (2009), That 'Internet of Things' Thing, *RFID Journal*, , 22, p. 97-114, http://www.rfidjournal.com/article/view/4986, last seen October 21st, 2013.

[16] For a more clear explanation on the way RFID works see http://www.scienceprog.com/how-does-rfid-tag-technology-works/, last seen November 29 th, 2012.

[17] A non-profit organization leading the development of industry-driven standards for the Electronic Product Code.

[18] See http://www.rfidjournal.com/article/articleprint/3940/-1/1/, last seen January 10th, 2013

[19] European Parliament resolution of 15 June 2010 on the Internet of Things, consideration 16.

[20] Cluster of European Research Projects on the Internet of Things, *Visions and Challenges for Realising the Internet of Things*, European Union, March 2010.

[21] See http://cordis.europa.eu/fp7/understand_en.html, last seen January 4th, 2011.

[22] See http://www.intertradeireland.com/fp72012/Commissioners%20Speech.pdf , last seen January 4th, 2013.

[23] FP7 in Brief, How to get involved in the EU 7th Framework Programme for Research, European Communities 2007, p. 7.

[24] In the right column a '+' is used whenever there is an extra domain. Aerospace and aviation is the only category I used twice, as this seems to be applicable to transport as well as space. Compare FP7 in Brief, p. 14 with CERP *Visions and Challenges for Realising the Internet of Things*, p. 41-42.

[25] This is a very wide category that can encompass a lot of domains. I limited myself to these three.

[26] See http://cordis.europa.eu/fp7/transport/home_en.html, last seen November 29 th, 2012.

[27] The Internet of Things: ITU Internet Reports 2005, p.12.

[28] See http://blogs.ec.europa.eu/neelie-kroes/ecall-using-ict-to-save-lives/#more-753 , last seen January 10th, 2012.

[29] This example suits the IoT concept as put forward by CASAGRAS, since it can be framed as a network development that will offer specific object-identification, sensor and connection capability that can serve as the basis for the development of independent cooperative services and applications.

[30] See http://www.ertico.com/heero, last seen January 24th, 2013.

[31] See http://bit.ly/nG5gLT, last seen November 29th, 2012.

[32] See http://cordis.europa.eu/fp7/ict/, last seen November 29th, 2012. The Cooperation programme itself is the biggest specific programme within FP7, with a budget of €32.413 billion

[33] ICT - Information and communication technologies, *Work programme* 2013, Cooperation theme 3, (European Commission C (2012)4536 of 09 July 2012), p. 8. See http://bit.ly/WYHmDL, last seen January 24th, 2013.

[34] See http://www.srdc.com.tr/projects/icardea/ & http://bit.ly/S9nCk0, last seen January 17th, 2013.

[35] M. Friedewald, R. Lindner & D. Wright (2006), *Safeguards in a World of Ambient Intelligence (SWAMI)*

Threats, Vulnerabilities and Safeguards in Ambient Intelligence , Deliverable D3, 3 July 2006, p. 37.

[36] SWAMI, p. 8 & 25.

[37] A report from the EU Commission Task Force claims that smart meters are necessary to realize a smart grid. The Task Force for Smart Grids Expert Group 1, *Functionalities of smart grids and smart meters*, December 2010, p. 16.

[38] 'Smart Grids: from innovation to deployment' (Brussels 12.4.2011: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of theRegions, 2011) see http://bit.ly/KVVKWW, last seen January 25th, 2013.

[39] Council Directive (EC) 2009/72 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC [2009], OJ L 211/55, (2009 Electricity Directive).

[40] European Commission, Information Society and Media Directorate-General & Energy Directorate-General, *Set of common functional requirements of the SMART METER*, October 2011.

[41] J. Arko, *Building the Internet of Things*, Ericsson Research, p. 1. See http://www.arkko.com/publications/vitel_arkko.pdf, last seen August 18th , 2012.

[42] F.D. Garcia & B. Jacobs, *Privacy-friendly Energy-metering via Homomorphic Encryption*, Institute for Computing and Information Sciences, Radboud University Nijmegen, p. 4.

[43] Task Force for Smart Grids Expert Group, p. 15.

[44] Smart meters can be used for gas, water and electricity. The scope of this article is limited to the smart electricity meter, so this is what the term 'smart meter' refers to for the rest of the article.

[45] Cluster of European Research Projects on the Internet of Things, *Visions and Challenges for Realising the Internet of Things*, March 2010, p 51. Hereafter defined as *Intelligent Home Network*, IHN.

[46] Mulligan, Deirdre K., Wang, Longhao, and Burstein, Aaron J.. University of California,

Berkeley. 2010. *Privacy in the Smart Grid: An Information Flow Analysis.*California

Institute for Energy and Environment. Final Project Report, p. 41.

[47] ICT - Information and communication technologies, *Work programme* 2013, Cooperation theme 3, (European Commission C (2012)4536 of 09 July 2012), p. 37 & 44. See http://bit.ly/WYHmDL, last seen January 24th, 2013.

[48] This is the number I got through correspondence with an EU representative closely involved in CERP IoT.

[49] The realizing of the smart grid which can be brought under the scope of the IoT-vision already receives € 300 million.

[50] This group consisted of 27 people, among which were the representatives of the industrial defense-lobby:Jan Dekker of TNO, Thomas Diehl of Diel Stiftung & Co (producer of the 'Sidewinder rocket' and 'Panzerfaust 3'), Pier-Francesco Guarguaglini of Finmeccanica, Rainer Hertrich of EADS (a Dutch NV that has divisions in airbus, military transport aircraft, aeronautics, space and defence and security systems), Erik Löwenadler of Ericsson Microwave Systems, Javier Monzón of INDRA (a Spanish information technology and defense systems company), Denis Ranque of Thales, Mike Turner of BAE-systems and Claus Weyrich of Siemens.

[51] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *Security Research: The Next Steps*, Brussels 7.9.2004, COM (2004) 590 final.

[52] This phrase is literally cited from page 6 of the 'Research for a Secure Europe: Report of the Group of Personalities in the field of Security Research.'

[53] Security Research, Towards a more secure society and increased industrial competitiveness, Security Research Projects under the 7th Framework Programme for Research, European Commission, May 2009, p. 3.

[54] See http://ec.europa.eu/enterprise/policies/security/indect/index_en.htm , last seen January 25th, 2013.

[55] See http://wlstorage.net/file/indect-deliverable-4-2009.pdf, last seen January 25th, 2013.

[56] See http://www.indect-project.eu/, last seen January 25th, 2013.

[57] See http://www.sikharchives.com/?p=287, last seen January 25th, 2013. In case of doubt, I can mail the original pdf.

[58] SWAMI, p. 11.

[59] See http://bit.ly/8ZFORy, last seen January 25th, 2013.

[60] M. Los, 'Looking into the future: surveillance, globalization and the totalitarian potential', in *Theorizing Surveillance: The panopticon and beyond*, ed. D. Lyon (Devon: Willan Publishing, 2006), p. 73.

[61] Bentham, Jeremy. Panopticon (Preface). In Miran Bozovic (ed.), *The Panopticon Writings*, London: Verso, 1995, p. 29-95.

[62] See http://bit.ly/11ytGVC, last seen November 29th, 2012.

[63] European Commission, Information Society and Media Directorate-General & Energy Directorate-General, *Set of common functional requirements of the SMART METER*, October 2011.

[64] B. Schermer, *Surveillance and Privacy in the Ubiquitous Network Society*, Amsterdam Law Forum, Vol. 1, No. 4, 2009, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1509360.

[65] L. Lessig, *Code and Other Laws of Cyberspace*, (Basic Books, New York 1999), p. 4.

[66] See http://www.uitzendinggemist.nl/afleveringen/1243625, between 20:20 and 21:40, last seen January 20th, 2013.

[67] See http://bit.ly/VeLZf2, p. 1 of the report, last seen January 25th, 2013.

[68] See http://www.eu2007.de/en/News/Press_Releases/May/0521BMI.html, last seen August 17th, 2012.

[69] PUBLIC SECURITY AND TECHNOLOGY IN EUROPE: MOVING FORWARD, Concept paper on the European strategy to transform Public security organizations in a Connected World, p. 8. See http://bit.ly/PqvWIJ, last seen August 17th, 2012.

[70] See http://bit.ly/w0wg0K, last seen August 17th, 2012.

[71] See http://cas.okstate.edu/jb/faculty/senat/jb3163/infoprivacy.html, last seen January 25th, 2013.

[72] See http://ec.europa.eu/justice/data-protection/index_en.htm, last seen January 11th, 2013.

[73] Consideration 2 of the Data Protection Directive.

[74] See http://ec.europa.eu/justice/data-protection/index_en.htm, last seen January 11th, 2012.

[75] For this article I leave the right to respect for family life, the home and correspondence outside of the scope.

[76] Bentham, Jeremy. Panopticon (Preface). In Miran Bozovic (ed.), *The Panopticon Writings*, London: Verso, 1995, p. 29-95.

[77] Kafka his books display what happens if this control is lost. ……

[78] Cluster of European Research Projects on the Internet of Things, *Visions and Challenges for Realising the Internet of Things*, March 2010, p 57.

[79] Cluster of European Research Projects on the Internet of Things, *Visions and Challenges for Realising the Internet of Things*, March 2010, p 57.

[80] H. Arendt, *Over geweld (On Violence)*, Amsterdam: Atlas 2004, p. 110.

[81] Council Directive 95/46 (EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995], OJ L 281/31.

[82] Article 6 (b) Data Protection Directive.

[83] Council Directive 2006/24 (EC) on the retention of data generated or processed in connection with the provision of publicly available communication services or public communication networks and amending Directive 2002/58/EC[2006], OJ L 105/54.

[84] Art. 1 Directive 2006/24 (EC).

[85] See http://huff.to/Y14oMZ, last seen January 24th, 2013.

[86] Swami, p. 37.

[87] Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU), [2012] OJ L 73/9, p. 11. See http://bit.ly/A0zXvf, last seen January 24th, 2013.

[88] Council Directive 2002/58 (EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37.

[89] See http://bit.ly/McWK9V, last seen August 18th, 2012.

[90] European Parliament resolution of 15 June 2010 on the Internet of Things, paragraph E.

[91] The World Market for Smart Home Energy Management Systems - 2012 edition, p. 3. See http://bit.ly/PBEw7A, last seen August 18th, 2012.

[92] Mulligan, Deirdre K., Wang, Longhao, and Burstein, Aaron J. University of California,

Berkeley. 2010. *Privacy in the Smart Grid: An Information Flow Analysis.*California

Institute for Energy and Environment. Final Project Report, p. 41.

[93] Vincent Icke, 'Gullivers Web', see http://bit.ly/WiQZ3r, last seen January 10th, 2012.