Professional report no. 5-2017

Dag Slettemeås, Ardis Storm-Mathisen and Jo Helle-Valle

RFID in Society
- Preparing for the Internet of Things
Final Report & Summary

(deliverable 4 of 4)

SIFO
Consumption Research Norway
OSLO AND AKERSHUS
UNIVERSITY COLLEGE
OF APPLIED SCIENCES

Professional report no 5 – 2017

CONSUMPTION RESEARCH NORWAY - SIFO
OSLO AND AKERSHUS UNIVERSITY COLLEGE OF APPLIED
SCIENCES Stensberggt. 26.

PO BOX 4, St. Olavs plass, NO-0130 Oslo, NORWAY

www.hioa.no/sifo

SIFO
Consumption Research Norway
OSLO AND AKERSHUS
UNIVERSITY COLLEGE
OF APPLIED SCIENCES

Professional report nr. 5-2017

Title RFID in Society – Preparing for the Internet of Things. Final Report & Summary (Del. 4 of 4)	**Antall sider** 41	**Dato** 25.09.2017
	ISBN 82-7063-467-0	**ISSN**
Authors Dag Slettemeås, Ardis Storm-Mathisen, Jo Helle-Valle	**Prosjektnummer** 416006	**Faglig ansvarlig sign.** Torvald Tangeland

Financed by

Norges forskningsråd / Research Council of Norway

Summary

This is the final of four project reports stemming from the RCN-financed project *RFID in Society – Preparing for the Internet of Things* (2010-2017). In addition to articles, conference papers, an exhibition, presentations, media contributions and a project website, the project has published the following reports:

Del. 1 of 4: "Case Criteria & Selection"
Del. 2 of 4: "Case Analyses & Evaluation"
Del. 3 of 4: "Handbook of Methods"
Del. 4 of 4: "Final Report & Summary"

The *RFID in Society* project has truly been a knowledge-building project. The project has, through a cross-disciplinary approach (although with more focus on social science perspectives than technical perspectives and design), explored a range of different cases, methodologies, and methods of analysis – all with the aim of providing a better understanding of the RFID/IoT phenomenon and its potential future position in society. The outcome of the research can inform Norwegian research/innovation efforts as well as policy/organised interests when manoeuvring in the RFID/IoT field. From the project initiation until present day, we see that the discourse around IoT has changed. Starting from a very industry-focussed "ICT" domain, with RFID being the prime figure and key enabler for a future Internet of things, we have seen a dramatic reorientation towards consumer and societal application areas. With this has come the dwindling role of RFID (at least in consumer-related application areas) at the expense of a wide array of technologies that make things and environments "smart", "intelligent" and "connected".

In terms of applications aimed at the consumer-citizen, we see a particular dramatic surge in smart consumer products, smart electronics, connected cars, wearables/smart health applications, smart homes, smart advertising. Hence, the primary tech-consumer domain in the early phase – RFID in retail – has somewhat lost momentum (at least at the consumer end), while smart products have pushed forward (somewhat skipping retail, and enabling a more direct producer-consumer engagement). Now, the key enabler (for consumers) is the smartphone, with a range of communication capabilities towards smart environments (using Wi-Fi, Bluetooth, NFC, apps, embedded sensors, etc.). Both the technological and the cultural premises have thus changed over the years, with consumers becoming considerably more *active in "building" the IoT* through direct participation (and consequent data generation) via their smartphones and smart-things – feeding the IoT with an exponential data stream. A major part of the potential for value-creation is identified in this IoT/Big Data symbiosis.

Still, even with consumers engaging more vividly with IoT-type services and applications, research finds that *consumer awareness* is still low regarding the concept itself. We are still at a stage where IoT is more prevalent on the "discursive level" than on the "tangible-things" level. There is an inherent paradox of IoT, being part of two interlinked but conflicting developments; the *data-driven economy* and a stricter *privacy framework*. This "technology paradox" associated with IoT is still not solved, and will continue to boggle the minds of innovators and politicians in the years to come. In this landscape of a global technological disruption and pervasive technology development – affecting the whole of society – the *RFID in Society* project is merely one building block in terms of getting to grips with, and seeking to understand the impact of, the evolving Internet of things.

Keywords

Internet of things, IoT, RFID, privacy, technology paradox, connected/smart things

RFID in Society – Preparing for the Internet of Things.
Final Report & Summary (Del. 4 of 4)

by

Dag Slettemeås, Ardis Storm-Mathisen & Jo Helle-Valle

2017

Forbruksforskningsinstituttet SIFO, Høgskolen i Oslo og Akershus
Postboks 4 St. Olavs plass, 0130 Oslo

Acknowledgements

This report is the final project report in a series of four. It addresses the overall achievements of the RCN-financed project «RFID in Society – Preparing for the Internet of things». It also positions the research in the present IoT environment, and reflects on the phase prior to project start-up. The project was initiated in 2010, with a project period of three years. Due to unforeseen circumstances at two of the research facilities partaking in the project, the finalisation of the project has been delayed several times, with final completion in September 2017.

The project group decided that even though much of the work has been carried out in different time periods, the project reports (deliverable 1 to 4) should be published at the same time. In this way minor and major alterations could be implemented along the way in order to make the reports as connected and up-to-date as possible. This is particularly important when exploring new and evolving technologies and paradigms such as RFID and the Internet of Things. This report is authored by Dag Slettemeås (SIFO/HiOA), with contributions from Ardis Storm-Mathisen and Jo Helle-Valle (SIFO/HiOA).

Oslo, September 2017

Forbruksforskningsinstituttet SIFO
Høgskolen i Oslo og Akershus

Content

Summary

This is the final of four project reports stemming from the RCN-financed project *RFID in Society – Preparing for the Internet of Things* (2010-2017). In addition to articles, conference papers, an exhibition, presentations, media contributions and a project website, the project has published the following reports:

Del. 1 of 4: “Case Criteria & Selection”
Del. 2 of 4: “Case Analyses & Evaluation”
Del. 3 of 4: “Handbook of Methods”
Del. 4 of 4: “Final Report & Summary”

The *RFID in Society* project has truly been a knowledge-building project. The project has, through a cross-disciplinary approach (although with more focus on social science perspectives than technical perspectives and design), explored a range of different cases, methodologies, and methods of analysis – all with the aim of providing a better understanding of the RFID/IoT phenomenon and its potential future position in society. The outcome of the research can inform Norwegian research/innovation efforts as well as policy/organised interests when manoeuvring in the RFID/IoT field. From the project initiation until present day, we see that the discourse around IoT has changed. Starting from a very industry-focussed “ICT” domain, with RFID being the prime figure and key enabler for a future Internet of things, we have seen a dramatic reorientation towards consumer and societal application areas. With this has come the dwindling role of RFID (at least in consumer-related application areas) at the expense of a wide array of technologies that make things and environments “smart”, “intelligent” and “connected”.

In terms of applications aimed at the consumer-citizen, we see a particular dramatic surge in smart consumer products, smart electronics, connected cars, wearables/smart health applications, smart homes, smart advertising. Hence, the primary tech-consumer domain in the early phase – RFID in retail – has somewhat lost momentum (at least at the consumer end), while smart products have pushed forward (somewhat skipping retail, and enabling a more direct producer-consumer engagement). Now, the key enabler (for consumers) is the smartphone, with a range of communication capabilities towards smart environments (using Wi-Fi, Bluetooth, NFC, apps, embedded sensors, etc.). Both the technological and the cultural premises have thus changed over the years, with consumers becoming considerably more *active in “building” the IoT* through direct participation (and consequent data generation) via their smartphones and smart-things – feeding the IoT with an exponential data stream. A major part of the potential for value-creation is identified in this IoT/Big Data symbiosis.

Still, even with consumers engaging more vividly with IoT-type services and applications, research finds that *consumer awareness* is still low regarding the concept itself. We are still at a stage where IoT is more prevalent on the “discursive level” than on the “tangible-things” level. There is an inherent paradox of IoT, being part of two interlinked but conflicting developments;

the *data-driven economy* and a stricter *privacy framework*. This “technology paradox” associated with IoT is still not solved, and will continue to boggle the minds of innovators and politicians in the years to come.

In this landscape of a global technological disruption and pervasive technology development – affecting the whole of society – the *RFID in Society* project is merely one building block in terms of getting to grips with, and seeking to understand the impact of, the evolving Internet of things.

1 Introduction

This is the final of four project reports stemming from the RCN-financed project *RFID in Society – Preparing for the Internet of Things* (2010-2017). In addition to articles, conference papers, an exhibition, presentations, media contributions and a project website[1], the project has published the following reports:

Del. 1 of 4: “Case Criteria & Selection”
Del. 2 of 4: “Case Analyses & Evaluation”
Del. 3 of 4: “Handbook of Methods”
Del. 4 of 4: “Final Report & Summary”

Before presenting the content of this fourth report, we provide a brief background of the main project itself.

1.1 Short introduction to the *RFID in Society* project

The project *RFID in Society – Preparing for the Internet of Things. Researching Opportunities and Obstacles in RFID innovation (or short: RFID in Society)* is funded by the Research Council of Norway (RCN) under the VERDIKT programme. VERDIKT (*Kjernekompetanse og verdiskaping i IKT*) has had a total budget of 1.2 billion NOK in the period 2005-2014. In mid-2010, 204 million NOK was awarded to 21 projects within the areas of social networks, Internet of Things (IoT) and mobile internet. The *RFID in Society* project received funding as a “researcher project” (*forskerprosjekt*) under this call. SIFO[2] has been leading the project, and TIK (UiO)[3] and IMK (UiO)[4] and SNF (NHH)[5] has been project partners. The project commenced in 2010, involved a two master projects (TIK, NHH) and a post-doc position (TIK), and was completed in September 2017 (delayed due to unforeseen circumstances).

The backdrop for this project is the rapid growth in applications for RFID[6] and sensor technology, and the emerging vision/paradigm of a future *Internet of things* (IoT). IoT has recently become a central theme in European and Norwegian ICT research politics, while RFID and other enabling technologies (sensors, actuators, etc.) are considered to be key components in a global IoT system. Advocates project vast economic opportunities and societal gain from IoT-development, while critics see enormous challenges (privacy, security, disruption, social effects, etc.) inherent in this technological move.

[1] Cf.: https://rfidsociety.wordpress.com/
[2] SIFO – Forbruksforskningsinstituttet, Høgskolen i Oslo og Akershus: http://www.hioa.no/Om-HiOA/Senter-for-velferds-og-arbeidslivsforskning/SIFO
[3] TIK – Senter for teknologi, innovasjon og kultur, Universitetet i Oslo: http://www.sv.uio.no/tik/
[4] IMK – Institutt for medier og kommunikasjon, Universitetet i Oslo: https://www.hf.uio.no/imk/
[5] SNF – Samfunns- og næringslivsforskning, Handelshøyskolen i Bergen: http://www.snf.no/
[6] RFID – Radio-frequency identification

Hence, the aim of the project was to address this situation. It set out to study how novel technologies (such as RFID) and emerging paradigms (such as IoT) can affect individuals/consumers and community/society. This implied a focus on "people-centric" applications of relevant technology and policy, while addressing both opportunities and challenges when such technology enter everyday life. SIFO had already, in late 2000, addressed the emerging consumer aspects or RFID/IoT in conferences (Slettemeås 2007a), to policy/government (2007b) and journal articles (Slettemeås 2009). At the time of project initiation, research (in particular in the Norwegian context) on individual/societal consequences of RFID/IoT was scarce, and had so far not properly addressed the socially complex and many-faceted nature of this type of technology and its relationship to social environments.

The project proposed that new approaches where needed in order to understand the role and function of RFID/IoT in society, and how this technology in the future may radically affect economic and social life. The aim was to develop several methods for studying such innovations from different practical and theoretical perspectives, primarily by identifying relevant cases to be studied (pilots, actual applications, future visions). The outcome of this research aspire to support future Norwegian research/innovation as well as policy/organised interests when manoeuvring in the RFID/IoT field.

1.2 Background for this report (del. 4 of 4)

The purpose of the report is to summarize the various research-related efforts and achievements of the *RFID in Society* project as a whole. We initiate the report by reviewing the development of RFID/IoT over the years, in particular the changes experienced in the project period (2010-2017). As the project finalisation has been postponed due to unforeseen circumstances, the upside has been the opportunity to capture the latest developments and changes that have occurred over the last few years.

1.3 A note on technology

As in report 1 and 2 we first provide a brief introduction to how we have approached the "relevant technology" in this project. In order to delimit the study it was crucial to identify the technologies that appeared to be relevant. In the project (and in the project application process), we kept a relatively narrow focus on RFID (as this has been the most prevalent technology during the first decade of 2000, and the enabling technology that has symbolized the shift towards IoT). In recent years (2010 onwards), attention has shifted to include other relevant technologies. Hence, we have used the term *AIDC (automatic identification and data capture)* – a more general term – interchangeably with RFID.

The term AIDC implies systems that identify objects automatically, gather information from these, and finally enter and interpret these data in computer-aided systems. The key enabler for data exchange is some sort of data transfer technology. The most common of these are barcodes, QR[7]-codes (2D barcodes), OCR[8], RFID/NFC[9], BLE[10], in addition to biometrics, magnetic and smart cards, as well as iris and voice recognition[11]. While barcodes and QR-codes need to be scanned (e.g. with a mobile camera and integrated/downloaded scanning software), RFID and NFC implies automatic data transfer when relevant devices are within reading range. AIDC is also relevant in the Norwegian context, due to the application of this reference in the

[7] Quick Response
[8] Optical Character Recognition
[9] Near Field Communication
[10] Bluetooth Low Energy
[11] Cf. Wikipedia: https://en.wikipedia.org/wiki/Automatic_identification_and_data_capture

standardisation work in this area. SIFO, the project manager, became a member of the Standards Norway[12] committee *"SN/K 178 – Automatisk identifikasjon of datafangst"*[13] during the project period. This is a "mirror committee" for standardisation projects in *CEN/TC 225 Automatic Identification and Data Capture (AIDC) Technologies and Applications* and in *ISO/JTC 1/SC 31 Automatic identification and data capture techniques.* The group mandate was also to address the relationship between AIDCs (with primary attention on RFID) and other wireless and sensor technologies and networks. In addition, the group mandate was to relate this work to standardisation work within global unique identifiers and the future internet of things (IoT).

There are also other terms that embody practically the same types of technologies and functions. Still, much literature on the transfer of data from real life objects to digital systems have concentrated on radio-frequency technology. Hence, RFID has in many ways (until a few years ago) ended up as a "collective concept" for a range of resembling technologies. RFID is widely recognised and used internationally in academic, media and public debate. More recently, NFC has attracted attention as this technology has been implemented in new smartphone releases (i.e. for contactless payment and other service where smartphones are used for activating services in the proximity of the user). NFC is based on RFID technology, and data transfer can be automatically activated when reader (smartphone) and tags or other mobile NFC-devices are within a certain distance from one another. NFC demands a short reading distance and is usually practical for services that have higher demands in terms of security.

Presently, focus has shifted from these enabling technologies to IoT. A 2016 report by Rathenau Instituut[14] ("Beyond control: Exploratory study on the discourse in Silicon Valley about consumer privacy in the internet of things"), addressing the "hyper-connected consumer", lists the key technological elements of IoT[15]:

- *sensors* (give things context awareness, ability to collect data)
- *actuators* (enable things to perform actions in the physical world)
- *processing units* (on chip, give things capability to do small computing on collected data, operate without human intervention)
- *unique identifier* (ensures that things can be identified and found in the network)
- *communication and network technology* (connecting things to the internet, or to local network/gateway device between thing and internet)

In the *RFID in Society* project, we have mainly focussed on RFID and NFC[16] (in addition to QR-codes and GPS), as well as IoT as an overarching technological system that employs these enabling technologies.

1.4 Pre-project RFID engagement

Technically, RFID is a generic term (as stated above) for technologies that enable an item to be uniquely identified, and where the item can communicate its identity (and other data) to its surroundings through radio waves. The RFID system can in simple terms be said to consist of an RFID tag (transponder), with a tiny microchip and antenna, a reader (transceiver), and sensors and a database. The tag can be *active* (containing a battery), continually radiating information, or *passive* (energy generated from the reading device) (Slettemeås 2009).

[12] http://www.standard.no/en/

[13] https://www.standard.no/standardisering/komiteer/sn/SNK-178/

[14] Cf: https://www.rathenau.nl/en/publication/beyond-control

[15] Cf. p. 4: https://www.rathenau.nl/en/publication/beyond-control

[16] NFC has been relevant in terms of the *NFC City* project that has run in parallel with the *RFID in Society* project, and in which SIFO has also been a project partner.

RFID, in practical use, has a long history. It was used for military purposes, already identifying friendly aircrafts during World War II. From the 1980s it was used for tagging livestock and for managing car parts in car production. From the 1990s it entered the supply chain, for improving management and distribution systems, and for automated toll collection (cf. Slettemeås 2009 for a thorough review of RFID). Later, access control and patient/people and garment tracking, as well as tracing food, became relevant areas for RFID usage.

In mid-2000 there were developments, in the US, Germany and Asia in particular, indicating a burgeoning interest in using RFID "closer to the consumer". In retail there were attempts to introduce RFID for in-aisle consumer companionship, as a way to identify consumer shopping habits, for renewing coupon strategies, as well as for leaving products tagged with RFID ("live products") after purchase for potential post-sale services and as "integrated" receipts/warranties. In this way market actors saw a potential for new value-added services (due to increased potential for data harvesting after purchase) that could not be realised without this technology. There was also a potential for tying consumers closer to producers, retailers and products in order to build a stronger sense of loyalty.

In the late 2000s, as we were nearing the end of the first decade of the new century, researchers at SIFO (the project owner) started investigating the ongoing developments around RFID. Of interest was the increasing tendency of such technology to enable "connected" or "smart" objects and environments. In October 2007 (ten years back), SIFO addressed the topic of RFID at the *Nordic Consumer Policy Research Conference* in Helsinki, Finland. In presenting the paper (Slettemeås 2007a), SIFO pointed to the coming transition of tagging products with RFID, as a replacement of the well-known barcode. This allowed for unique identification of products, that additionally could communicate their ID and status to the world, and to the internet (through chip and antenna). Hence, previously "passive consumer products" could suddenly become "active", enabling them to be easily identified (at a distance), counted, tracked, and analysed digitally.

It seemed, at this point in time, that RFID (and related technologies) implied a potential *paradigm shift* in how consumers would come to interact with smart and connected/communicating objects and environments. The advantages seemed to be many (Slettemeås 2007a):

General advantages were assumed to be:

- Increased automation
- Unique identification
- Improved visibility
- Real-time information
- Enhanced product information
- Instant verification of products (trust)
- Improved efficiency/cost savings

In terms of more retail-specific advantages, these aspects were identified as:

- Post-sales services (product recall, notice of default, product upgrades)
- Deterring shoplifting
- Profiling of consumers according to interests and shopping behaviour
- In-aisle companion for product suggestions
- Instant recognition of preferences
- New marketing methods – more targeted and instant marketing based on predictions
- Less excess product inventory, and right products at the right time
- Addressing consumer demands for improved and more correct services
- Removing/reducing check-out lines through mobile RFID scanners used by consumers

At the same time, moving RFID from “behind the scenes” (i.e. in the supply chain) and to the forefront, interacting directly with consumers (by being attached to or embedded in products and services), *consumer and privacy concerns* started emerging. Some concerns were (Slettemeås 2007a):

- *Covert tracking* – consumer items being scanned from a distance, and consumers being ”spied on” through their communicating items.
- *Recordings of location* – when and where a consumer engages with specific products, products leaving ”information trails”.
- *Privacy invasion* – profile data about user potentially being coupled with instant data about user habits, based on info from RFID-enabled products that consumers engage with.
- *Price discrimination* – “deep” knowledge about consumers, generated through their objects, can generate price discrimination strategies.
- *Targeted marketing* – data generated from RFID product engagement, combined with user profiles, could lead to more tailored and targeted marketing. RFID could also be used for targeting marketing efforts (two-way potential).
- *Predictive capability* – by analysing previous habits, with data generated from RFID-products, market actors can anticipate consumer preferences or actions.

Hence, during the early 2000s, the *“Big Brother”*-label was emerging in public discourse, being directly connected with the RFID technology. Privacy and consumer advocates (especially in the US) drew pictures of a seamless network of millions of RFID readers, billions of tags placed everywhere, huge databases, tracking of consumer movements – and a constant reading, processing and evaluation of consumer data predicting consumer behaviour. This would eventually make real the nightmare of an inescapable, private sector-lead Orwellian surveillance, according to the RFID opponents. The Helsinki-paper (Slettemeås 2007a) thus suggested that the Norwegian government should gather knowledge based on the experiences, particularly from the US and Germany, to prepare for a similar development in the Nordic countries. In addition to consumer/privacy issues, it was suggested a “privacy-by-design”-orientation in RFID development, more coordinated research efforts, as well as cooperation between developers, researchers, regulatory authorities, consumer groups and privacy advocates.

The paper and presentation of consumer-oriented RFID (Slettemeås 2007a) marked the start of SIFO efforts to follow the RFID and IoT development. A policy report was written to the Ministry of Children and Equality in late 2007 (Slettemeås 2007b), addressing consumer issues related to RFID, IoT, robots and smart cars/homes. It pointed out that the increasing prevalence of “pervasive and omnipresent technology” would potentially radically change consumers’ everyday life. This implied a move from traditional engagement with “passive” tangible consumer/household objects/technologies, to engagement with “active” communicating service-objects, where processing power and network connectivity would be integrated in everyday technology and consumer objects.

The omnipresence of such technology would bring both positive and negative consequences to consumers, the report stated. Pervasive, but “hidden”, digital objects and environments can *support consumers* in their everyday life, but at the same time *reduce consumer reflection* on the consequences of such use, as they are not facing visible technology. Hence, their ability to take *independent, active and reflected choices* could gradually erode. In addition, more constant surveillance, observation and interpretation/prediction of consumer behaviour, would yield great challenges for consumers and society, according to the SIFO policy report (Slettemeås 2007b, p. 155). Two factors were addressed; *awareness* – what happens to consumers when decision power is decentralised or outsourced to technology?; and *responsibility* – where is responsibility placed when technology gradually makes more independent choices, based on interpretation of "consumer-generated" data? In the report, RFID was mentioned specifically as a class of technology that would contribute to a first step in the direction of connected objects/environments and the omnipresence of technology in society. RFID (and sensors) was, at the time, the enabling technology that fed the visions of *ubiquitous pervasive computing* and *ambient intelligence*. RFID was synonymous with taking internet to a new level – an internet of physical things (Internet of things), where everyday objects could communicate with each other, with systems, with people and with the internet (Slettemeås 2007, p. 156).

Based on the Helsinki paper (Slettemeås 2007a) and the report to the ministry (Slettemeås 2007b), a much-sited agenda-setting article was published in *Journal of Consumer Policy* in 2009 on the RFID/IoT topic; *«RFID – the next step in consumer-product relations or Orwellian nightmare? Challenges for research and policy»* (Slettemeås 2009). This article holds a consumer perspective, but has a more encompassing perspective and ambition, setting the agenda for RFID/IoT-based research and policy directions for the future. It introduces the technological history of RFID, its societal relevance, and how it presents a potential paradigm shift when things get digitally connected, paving way for the vision of an internet of things (Slettemeås 2009, p. 222). The article continues to cover the potential application areas for this technology, were *retail* at the time was seen to have a huge potential, with automated purchasing and service systems and product recall opportunities. German-based Metro Group, US-based Walmart, and UK-based Tesco all tested out RFID in the mid-2000s, for tracking products, shelf-management, consumer loyalty programs, and so on.

The article also covers the *privacy and consumer concerns* that this technology raises. In mid-2000, concerns of a comprehensive surveillance society was prevalent, with researchers and consumer advocates opposing the RFID-development (as stated previously). Key concerns with RFID was *technology omnipresence, invisibility, pervasiveness, invasiveness, reduced human control, the inability to log off, unclear responsibilities and accountability, and increased technology-human hybridisation (i.e. subdermal RFID tags).* In addition concerns were raised about *people being identifiable through their possessions* (data privacy, location privacy), and hence the *general tracking and predictive capabilities* of RFID systems.

The article then addresses regulations relevant to RFID, how RFID has been covered in mass-media, i.e. the controversy raised by privacy groups, i.e. the use of terms such as "spychip", "tracking device", "big brother bar code", and "mark of the beast" (Slettemeås, 2009, p. 231). The article finally covers consumer-related research on RFID, and concludes with the need for a policy/research agenda on RFID-related themes:

> "A conscious, and well-founded approach to RFID – and to ubiquitous and pervasive computing – is the key to preventing anything even resembling an Orwellian nightmare from materialising" (Slettemeås, 2009, p. 241).

The *RFID in Soceity* project sought to follow up on some of the themes and challenges that weas identified and highlighted in this previous groundwork.

2 From RFID to IoT – recent developments

What is interesting to note is that in the years prior to project start-up (between 2006 and 2008) there was a change in terminology and scope when it came to connected devices and ubiquitous computing. The EU moved from an RFID-focus in 2006-2008 to an IoT-focus from 2008 onwards (Slettemeås 2009, p. 229), choosing IoT as an *action plan for Europe*. In a short period of time, attention shifted from the specific RFID technology to the more elusive vision of an internet of things (IoT). It is clear that RFID (as a key enabling technology) paved the way for the notion of IoT, while RFID in the last few year has been gradually downplayed and is no longer a direct and integral part of the IoT-vision. This was also a time when other major technology changes were taking place; from 2007 onwards, both *social media* and *smartphones/apps* started becoming mainstream – today seen as natural "ingredients" for "building" the IoT (i.e. for harvesting, distributing and receiving data about "things").

Another starting-point for IoT (rather than the political) would be to look more practically at the first "*connected things"*. In terms of actual internet-connected consumer devices, a toaster that could be turned on and off over the internet in 1990 can be considered the first IoT device (presented at the 1989 INTEROP conference)[17]. The *concept* "Internet of Things" (IoT), however, also has a more technical origin. It is said to be coined by the Auto-ID Center director Kevin Ashton in 1999, in a presentation for Proctor & Gamble, where he linked together RFID and the internet when addressing the company's supply chain. He then, and still, means that computers and the internet are almost wholly dependent on people for information input, captured and created by people. At the same time, people are not very good at capturing data about things in the world. But, he claims that if data about things could be gathered without our help – where things could "see, hear and smell the world" – we could track and count everything and reduce waste, loss and cost. In 2009[18], Ashton still believed that RFID and sensors would contribute to change the world, and that RFID was not just a "barcode on steroids". The same year the *Auto-ID Lab* opened (the research-oriented successor to the MIT Auto-ID Center)[19]. It was here that the Electronic Product Code (EPC) was developed, the global RFID-based item identification system that intended to replace the Universal Product Code (UPC), or the barcode.

Still, even though IoT saw the first connected consumer product in 1990, was coined by Ashton as a concept in 1999, and became more widely used by the EU (in research and policy) from 2008 onwards, there is still no clear definition of IoT. In the last five years or so, the term has been used vividly in policy papers, and in mass and social media, with a wide range of conferences benefitting from the potentially far-reaching utopian or dystopian vision that the concept is associated with. This makes IoT highly interesting today, both as a "real" phenomenon and as a "discursive" or "media" phenomenon.

Below, we review some recent agenda-setting papers and stakeholder/policy documents that position IoT in today's context.

[17] Cf: https://www.postscapes.com/internet-of-things-history/
[18] Cf: http://www.rfidjournal.com/articles/view?4986
[19] Cf: https://www.postscapes.com/internet-of-things-history/

2.1 IoT – policy and societal issues

In a 2010 article, Atzori et al. (2010) survey the *internet of things* as a novel paradigm. The article states that in order to address and advance the field IoT, in its full reach and complexity, the combined effort of many different fields of knowledge is required. Hence, the article reviews different visions and approaches to IoT, as well as various enabling technologies associated with it. The authors state that the **effects of IoT** will be visible in both working and domestic fields (through domotics, assisted living, e-health, enhanced learning, etc). Benefits also comes with risks, and it is stressed that widespread adoption of IoT technology will lead to **everyday objects becoming information security risks**, and that the IoT can distribute those risks far more widely than the internet has done to date (Atzori et al 2010, p. 2787).

As several of the contributions below will repeat, this article also points out the difficulty of understanding what IoT really means (one paradigm, many visions), what the leading ideas behind the concept are, and the potential implications of full deployment of IoT on society. An apparent fuzziness is due to the name itself, it is stated, and that different organisations/sectors approach the concept from either an **internet-oriented** or **things-oriented** perspective. The authors describe that Internet of things semantically means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols, making relevant a third **semantic-oriented** perspective of IoT (Atzori et al 2010, p. 2788). We show this three-part definition of IoT below:

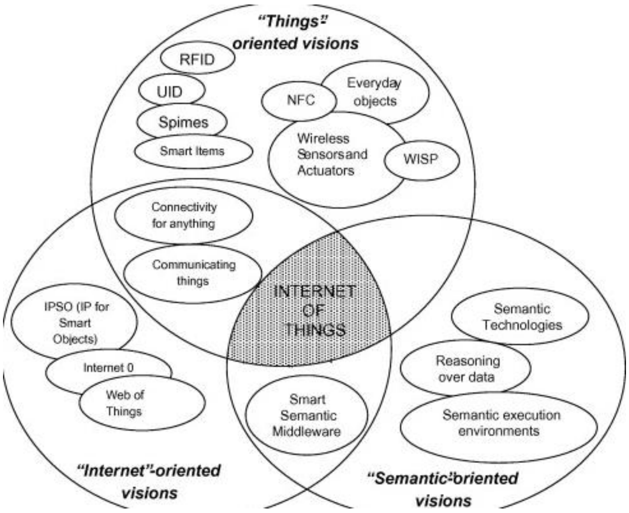

"Things"-oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensors and Actuators
WISP
Connectivity for anything
Communicating things
INTERNET OF THINGS
IPSO (IP for Smart Objects)
Internet 0
Web of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
"Internet"-oriented visions
"Semantic"-oriented visions

Figure 1: IoT in terms of a things-/internet-/ and a semantic-oriented perspective (source: Atzori et al. (2010)).

The authors point to the first attempts at defining IoT, in line with what *the RFID in Society* project centred on as a working definition, which was very much "things-oriented". Things were simple items – RFID tags – that could be attached to or embedded in products and environments, and IoT attributed to Auto-ID Labs, a global academic research network in the field networked RFID and sensing technologies. Together with EPC Global, a major focus have been to develop the Electronic Product Code (mentioned briefly in the previous sub-chapter), as well as to support the diffusion of RFID and industry-driven global standards. However, the authors claim IoT cannot be only be about the establishment of a global EPC system, where the only objects are RFID (or if RFID should be part of it at all, cf. the 2017 Ofcom report below). However, it is claimed that starting from RFID-centric solutions is fruitful, as the key capabilities of RFID (traceability and addressability) are central to IoT. Nevertheless, IoT must be more encompassing than "object identification" (Atzori et al 2010, p. 2788). A wider portfolio of devices, networks and service technologies will be needed to build the IoT, the author claim.

In a 2014 EU report[20] on research/innovation regarding IoT and cloud computing, IoT is considered a pervasive innovative technology building on the universal connectivity of things and people. It is already considered to be a reality (although many still claim it to be a mere vision) and the report expects IoT to be *the next big thing by 2020*; a fully hyper-connected society, with billions of IoT connections (as most of the things that can be connected is expected to be connected by then), and with full penetration of "IoT-communicators" among consumers/citizens (smartphones, tablets, etc.). It is stated that the concept of hyper-connectivity is interwoven with the idea of ubiquitous and pervasive computing, with sensors, actuators, and so on embedded in everyday objects, connected seamlessly together through a continuous network. IoT is described as related to other major technology developments such as *cloud computing* and *big data*. Both opportunities and barriers are summarized, and the report states that this new technology;

> "…is opening the new age of the hyper-connected society and acting as a powerful driver for business innovation, but also facing equally strong barriers in terms of security risks, concerns about privacy protection, and resistance to organizational change"[21].

The report believes that IoT is *not another "hype",* as specific cases are already found across many sectors. So far the development has been *mostly supply-driven*, but is now seeing *strong demand forces* (socio-economic trends, government initiatives, expanding consumer market), driving IoT towards a more **user-oriented situation**. The report sees the most attractive IoT business opportunities in smart manufacturing and smart health – but also in **smart homes** (home security, energy applications, household appliances, personal wellness applications, wearable devices) – that are becoming "**mini IoT environments**" – and through **smart customer experience** (retail-oriented; omni-channel operations, digital signage, in-store digital offers, NFC payment). Hence, for the EU, it is suggested to invest in technology for the *IoT-Cloud-Big Data combination*, to manage complexity, provide scalability, guarantee usability and preserve privacy by design. To bridge the gap between R&D efforts and the market – it is proposed that Europe must **develop a supply ecosystem**, and support massive adoption/critical user mass, both for industries and consumers. This includes *supporting skills, building trust and confidence* in emerging IoT economy, *removing regulatory barriers*, *ensuring security and interoperability*, and *encouraging cooperation*. This implies a necessary transition from a **product-centric** to a **service-centric** economy, and a tighter relationship between producers and consumers, overcoming the traditional dichotomy between technology (supply)-push and demand (consumer)-pull, favouring **user-driven collaborative innovation**.

It is expected that initially many IoT solutions and use-cases will have a strong vertical market component (industry focus), while the evolving IoT will require rethinking of the traditional horizontal platform/vertical segmentation, focusing on interconnectivity and interoperability – and orient itself towards smart (horizontal) environments (not vertical markets/industries). The report provides an example of home-based healthcare, which brings together smart solutions such as traditional tele-medicine, smart homes (domotics), smart buildings (environmental control and security), wearables (medical/fitness devices/clothing), assisted living solutions, and robotics[22].

Key benefits for consumers and individuals are expected to be *better customer experiences, increased transparency*, *reduced information asymmetry*, *timesaving, and reduced transaction costs*. For society as a whole one expect *more effective services*, *better use of public resources*, *reduced collective costs*, *enhanced environmental protection*, and *increased public safety and*

[20] 2014 EU report: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination

[21] 2014 EU report: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination

[22] Ibid.

security. As IoT creates new forms of contact, it becomes *harder for users to know, understand and control these new connections*. Thus, *classical market protection becomes less efficient* in human-to-machine and machine-to-machine interaction. It is suggested that, to amend this, trust must be built in emerging services, which goes beyond contractual obligations and regulation, improving awareness of potential benefits and risks around IoT services (such as privacy, autonomy, identity, and social inclusion).

In addition to this 2014 EU report, a ministry report from South Korea (*Master Plan for Building the Internet of Things)* published the same year, refers to the "hyper-connected" revolution based on IoT as a successor to the industrial and information revolutions[23]. It states that this is the very beginning of this revolution, with only 1% of objects currently being connected to the internet. The report envisions that **IoT will solve important issues and challenges in society**, in all sectors, and improve quality of life for citizens and consumers. There is still a phase with *high competition among global actors to develop a dominating platform and standards*, to take the lead through *building successful IoT ecosystems*. The goal is, however, an **open ecosystem** where it is easy to develop and provide services, and where in particular smartphones can be used for accessing IoT services.

In a 2016 OECD report[24], on the topic "tomorrow's Internet of things", discusses both opportunities and challenges in this development. It states that IoT refers to an ecosystem where *applications are driven by data collected from devices that sense and interface with the physical world.* Devices have communication connectivity, either direct connection to internet or mediated through local or wide area networks. It refers to an earlier OECD-report from 2011, where IoT was mainly associated with RFID-based applications (as we state in the introductory part of this report), while since 2011 IoT has become the more popular term, describing a wide variety of developments where things connect to the internet. The report points to four main elements in the development of IoT; a) **data analytics**, b) **cloud computing**), c) **data communication**, d) **sensors and actuators**[25]. A key aspect of IoT is also the ability to create "big data" ecosystems.

Soon, the report predicts, IoT can be as common as electricity in everyday life. It is the combination of *network connectivity*, *widespread sensor placement* and *sophisticated data analysis techniques* that now enable aggregation of enormous amounts of data by IoT devices in homes, public spaces, industry and the natural world, spanning almost all sectors. An IoT-"thing" can be an inanimate object that has been digitised or fitted with digital technology, as well as machines, animals or human bodies. The data gathered from these "things" can be used to discover patterns, predict changes or events, and change aspects of objects or environments. In terms of production processes, it enables *improved customization and less need for predicting mass market demand*. Machine to Machine (M2M) communication is seen as related to IoT, implying autonomous data communication with no human interaction between applications and devices, *facilitating automated decision and action*. **Internet of Everything (IoE)** is, according to the report, a more fitting term for this development, as internet-connected sensors and actuators do not only link to things, but can also monitor health, location, activities of people and animals, as well as monitor the environment, food quality, and so on.

The report states that the visions of communicating objects is not new, and that by the early 1990s ideas about ubiquitous and pervasive computing and embodied virtuality were commonplace, while the *popularity of consumer-product-IoT have taken longer than expected*. However, more IoT products are now reaching the stores (smart fridges, washing machines, clothes,

[23] 2014 Korean ministry report: http://www.kiot.or.kr/uploadFiles/board/KOREA-IoT%20Master%20Plan.pdf
[24] 2016 OECD report: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En
[25] Sensors are regarded as the interface between the physical world and the electrical devices. Actuators are conversely seen as converting electrical signals into a physical phenomenon (e.g displays)

toothbrushes, etc.), but still **manufacturers know little of what features will attract consumers**. The report compares IoT now to www[26] twenty years ago, an emerging commercial network, experiments across industries, competing standards and unclear consumer expectations. The difference from ten years back (the "RFID era"), is that with the wireless capabilities of smartphones, including NFC or BLE, and their widespread adoption – **everyone has devices that can communicate with the IoT** (directly with smart objects, feed smart objects/environments, or access IoT-services via internet). The OECD-report concludes that smartphones now play an important role in **"bringing the IoT to the consumer"**.

A 2017 Ofcom report (UK)[27], reviewing the latest developments in IoT (prepared by Cambridge Consultants), signals the British Ofcom priority to help and support the growth of IoT, creating a **healthy regulatory environment** to foster investment and innovation in IoT. Due to the lack of a standard definition of IoT, Ofcom has put forth five key criteria for IoT applications; 1) they must *embedded in everyday objects*, 2) use *embedded microprocessors*, 3) *connect via the internet*, 4) use *interconnected networks*, and 5) use *standardised communications*. Contrary to earlier definitions (that also the *RFID in Society* projects is founded on), the Ofcom definition excludes devices using wireless links, such as distributed sensors in burglar alarms, or RFID tags that enable objects to be identified and tracked. This proves the diversity of approaches in how to understand the IoT phenomenon.

The report identifies some main sectors for IoT growth; 1) **automotive/transportation**, 2) **consumer electronics and fast moving consumer goods (FMCG)** and 3) **utilities**. It expects that IoT, as a step-change technology, will move from a relatively "poorly understood technology" to become a "mainstay of many people's lives". However, it is stated, there is **no single IoT**. Rather, at least currently, **IoT is highly sector specific**, with little overlap and with a limited standardisation among IoT devices. The report is also aware of the often simplistic "counting" of number of connected devices to describe IoT development, and focusses attention on the "whole picture" – emphasising that IoT ecosystems are complex with many stakeholders affecting the IoT adoption-rate.

As with many other policy recommendations, this report also points to key policy roles of *securing informed choice*, *inspiring consumer awareness*, and *promoting secure-by-default design and consumer privacy*. In terms of **privacy**, the report claims that consumers have become aware of the many data privacy breaches of global companies, but that "consumer remain comfortable sharing information, as long as sharing it can be traded for some benefit"[28] (this point is somewhat problematic, as consumers seem to be less aware of (and worried about) the consequences of (partly covertly gathered) IoT data). Samsung, however, experienced reputational damage in 2015 after it was discovered that the voice-recognition system for its smart-TVs could capture private voice data, which were returned to Samsung for processing and monitoring.

In addition, much of **smart infrastructure and devices in homes are poorly protected**, allowing for potential malicious control of connected devices. There are default options and passwords, little possibility for upgrades, and, so far, little on-going commitment or customer service/relationship. Many devices and systems are also vulnerable to power outage. On top of this, the report states that many IoT products have so far been **lacking a clear and communicable consumer benefit.** Hence, it is concluded that IoT is still an immature phenomenon while public awareness is low. However, in 2016 in the UK, the **PETRAS Internet of Things Research Hub** was launched[29]. The hub is a collaboration between leading universities and business with the aim to explore critical issues relevant to IoT, such as privacy, ethics, trust,

[26] World Wide Web
[27] 2017 Ofcom report: https://www.ofcom.org.uk/__data/assets/pdf_file/0007/102004/Review-of-latest-developments-in-the-Internet-of-Things.pdf
[28] Ibid, p. 20
[29] Cf: www.petrashub.org

reliability, acceptability and security. The hub has more than 20 projects running across several application areas.

2.2 IoT – consumer and privacy issues

We already touched upon some privacy and consumer issues in previous chapter. In this subchapter we look at reports that primarily and directly addresses these issues in relation to IoT.

A 2016 report by *Consumers International* (CI 2016)[30], on IoT and challenges for consumer protection, addresses both the potential for new opportunities and risks for consumers. The main difference, if comparing traditional products and markets with IoT and connected objects and environments, is that consumers will experience a new and different relationships in the market. *Issues concerning compatibility, security, rights management and data collection, previously only affiliated with electronic devices (with software), suddenly applies to all kinds of traditional products and services – as dumb objects are fitted with smart accessories*. The disclosure and consent model governing digital products, could extend to a range of new products, as the boundaries between digital and physical items become blurred.

CI refers to various descriptions of IoT; that it will "change everything – including ourselves" (Cisco), and that it can potentially become one of the most "disruptive technologies we have ever experienced" as "everything that can be automated will be automated" (Pew). However, CI states that the term is now used so freely in both policy and business worlds, that identifying what it really means is futile. But, it often involves the idea of physical objects containing embedded sensing and communication technology, which enables the objects to interact with its surroundings and the internet. A particular feature is that it is no longer just "traditional" electronic devices that are connected in a network, but that "everyday" and previously "dumb" objects, devices and appliances suddenly have the capabilities to *compute, connect and communicate* (CI 2006, p.7). Furthermore, it is not only "things" that are connected, but also larger scale systems (electricity grids, transport networks, water systems, etc.), as well as people and animals (also stated in previous reports). The key feature is that the *thing, system or service* needs a *separate, recognisable identity* (address).

From a consumer perspective, the many aspects that have accelerated the trend towards IoT expansion (Wi-Fi/Bluetooth/NFC-connectivity, the IPv6 protocol, the coming 5G network, sophisticated sensors, improved battery quality, advanced data handling technology, cloud technology) are all factors that operate "behind the scenes" to promote IoT, according to CI. And consumers use their smartphones (the visible and tangible device that alter consumers' relationship with this expanded connectivity) as a "hub" to connect to smart devices and systems. Over time, the smartphone has "familiarised" people with performing a range of activities from a single device (CI 2006, p.14), preparing them for future engagement with/within IoT.

The main opportunities that can benefit consumers through IoT are identified as (CI 2016, p.24);

- **More responsive services** that can observe, learn, anticipate and respond to individuals' needs
- **Shorter feedback loops** as companies can quickly learn and respond to consumer experiences with products/services (real-time feedback from usage)
- **Increased convenience** through automated solutions, simple user interfaces, and time and cost savings
- **Enhanced experiences** through instant services that add to traditional experiences

[30] Cf: http://www.consumersinternational.org/media/1292/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf

- **Decision-making support** where knowledge can be acted upon directly by users, or be outsourced to automated service system (through predictions based on data analytics)
- **Better insights into own behaviour** through analysis of habits, usage patterns, time spent on tasks, etc.
- **Increased efficiency gains** for businesses that can be passed on to consumers
- **Offline security and safety** through geo-location tagging of items, access, etc.
- **Product verification** through IDs/authentication, preventing theft, counterfeiting, etc.
- **Remote controlling** of homes, appliances, etc.

Areas of concern with multiple connected devices have been identified as;

(Exacerbation of pre-existing issues, CI 2016, p. 28)

- **Lack of transparency and clarity** as products/devices link to multiple systems and carry out new functions. This makes it increasingly more difficult for consumers to have full clarity of how they work, leading to increased information asymmetry between consumers and producers.
- **Complex liability and responsibility chains.** Although interconnected service environments may increase convenience and sense of seamlessness- removing friction and hassle – identifying what/who is liable if something goes wrong becomes increasingly difficult.
- **Data collection and use** is scaled up. With increasing amounts of data being collected, aggregated and merged with other data, privacy and data protection is increasingly challenged (increased pressure on *informed consent* and *data minimisation*). In addition, IoT devices are (often) designed to communicate with each other and transfer data autonomously, making it difficult for consumers to see if, when and how data processing takes place.
- **Security** issues become even more prevalent in IoT environments. Hacking and disruption of services is not new in the digital world, but becomes more serious as consumers face the potential for i.e. hacked cars and home security systems, or even attacks on health devices or everyday products. Many IoT devices are designed without the ability for upgrades.

(New emerging issues, CI 2016, p. 33):

- **Development of hybrid products** where everyday tangible objects suddenly have digital properties embedded (software, communication capabilities), giving them additional functionalities. Questions arise, such as which part of the product will be licenced via contract (due to software), and which part will be owned (or rented), such as the physical item itself?
- **Erosion of ownership norms** as traditional non-digital products take on a new characters, becoming embedded with chip/software/communication. Software (classed as IPR[31]) often employ technological protection measures (TPMs) to prevent interference, blocking unauthorized access or modification (cf: DRMs[32]/digital locks, EULAs[33]). This affects both consumers' expectations and their actual behaviour regarding what they can and cannot do with their own products – as parts of the product function is licenced to consumers. These limit length of product support, enable sudden disablement of features/functions, block access, stop/enable programs from running/being downloaded, and enable remote data-wiping (through contract enforcement).
- **Lock-in to products and systems** limiting interoperability and portability. As more products get IoT features – and licenced use (as seen above) – consumers will be locked to vendors' ecosystem of products and systems. This limits opportunities for "shopping

[31] Intellectual property rights
[32] Digital Rights Management
[33] End User Licence Agreements

around" for other apps/services/repair opportunities, and the ability for modifications/tinkering/reverse-engineering. Similarly, it is difficult for consumers to move between providers, and to access and bring their own data with them (data portability) – and also to realise the utility value of their data (which in IoT systems will be coupled with new data for enhanced value).

- **Lock out of alternatives** leaving less choice for consumers to influence IoT by choosing not to participate. Easier to shift between suppliers than to opt out entirely (lack of "analogue" alternatives or experiencing direct/indirect penalties for non-participation).

Consumer protection mechanisms challenged:

- The **"caveat emptor"** principle (let the buyer beware), stemming from the fact that buyers have less information while the seller has more information about the good/service sold/purchased (information asymmetry), is under pressure with IoT. The **"disclosure and consent"** mechanism (in particular in the market for digital products) places a heavy burden on consumers to inform themselves (about terms, conditions – and data handling – of every transaction performed). Research reveals that *consumers spend very little time reading T&Cs before consenting to services*, while these T&Cs are often extremely comprehensive. At the same time, with IoT, the consumer will be "online" or "logged on" constantly, engaging continuously in and out for interactions and contracts, with less insight into what type consent is given, and for what purpose. On the other hand, this contrasts the fact that IoT produces an immense potential for **consumer-centred empowering applications**.

In the chapter *"The internet of whose things?"* (CI 2016, p. 50) the report asks who gets to decide what is to be connected, how information is used, what scope there is for meaningful choices once in the system, and whether or not to interact with pervasive systems. IoT development is, like much other development, driven by industries and the fact that "it can be done", rather than by thorough social and ethical evaluations of real needs. The report states that attention is often given to IoT in terms of how many things an people are connected, how fast it is, the money invested, potential efficiency gains – rather than to focus on the potential social endpoints of such projects. This implies grand questions such **what do we as a world seek to achieve through such technological innovation** (going further than mere privacy/security evaluations). With this comes the questions of **where the input and voices from consumers, citizens and future generations are**, and how careful considerations of all types of implications (in particular issues of control and agency) can be addressed without being interpreted as luddite or stifling innovation. In an increasingly connected society, it is suggested, the boundaries of acceptable practice and accountability should be designed in cooperation with citizens.

Another 2016 report[34] from the *Australian Communications Consumer Action Network (ACCAN)* on the connected home/human/habitat (Vulkanovski 2016) refers to IoT as a buzz phrase with no official definition. References are made to concepts such as "smart cities" (IBM), "industrial internet" (General Electric), "Internet of everything" (Cisco), and "the Internet of your things" (Microsoft). However, for IoT, the ISO definition is the one preferred in the report; "an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react" (Vulkanovski 2016, p.10). In addition there are overlapping concepts, such as machine-to-machine communication (M2M), cloud computing, and big data – where **IoT is an enabler of big data** (more "things" collecting data), while ubiquitous/pervasive computing ("everyware") enables connected things to become intuitive and autonomous.

The report also refers to measures of IoT development in terms of **"value"** (potential future value of services) and **"size"** (number of connected devices). In 2008-2009 Cisco calculated

[34] 2016 ACCAN report: https://accan.org.au/files/Reports/HomeTweetHome_IoT_Report-v2.pdf

that the number of things exchanging data on the internet exceeded the number of people, and hence proclaimed 2009 to be **“the birth of the internet of things”.** The report states that the future of IoT can be either **utopian or dystopian**, but will probably fall somewhere in-between, and that a **public IoT body** should oversee the development and conduct research on IoT in the market for the benefit of the public and policy. The relevant IoT issues identified in the report are placed in three consumer-oriented use cases;

1) **Connected Homes** (smart homes and appliances)
2) **Connected Humans** (personal wearables and health services)
3) **Connected Habitats** (smart cities and smart cars)

The report claims that the future of the connected *home, humans and habitat* lies not in the spectacular, but rather in *the familiar* – that it will *operate seamlessly in the background* and support our actions and decisions. The report identifies a range of broad IoT consumer issues based on the three use-cases, such as *privacy, security, interoperability, serviceability, consumer protection, affordability, choice and control, changing consumerism, environmental implications, and implications for specific groups* (e.g. for children, elderly, and disabled – enabling enhanced accessibility and participation in social/cultural life).

A main point in the report is that **consumer confidence is critical** for healthy uptake of IoT products and services. Consumers, it is predicted, will demand private and secure digital services. Hence, such services should embed “privacy/security by design” – giving consumers tools to control personal information, while adopting data minimisation policies. Opting-out of specific features and services, incremental consent for IoT services, and turning “smart” things “dumb” again are desired features. In addition, **interoperability** is a critical issues as well as **consumer education** on several IoT-related aspects (operation, data collection, potential inferences drawn from data, consumer tools, risk mitigation, etc.). A key conclusion is that: **“an informed consumer is an empowered consumer, and an informed and empowered consumer base can shape an ideal IoT consumer market”** (Vulankovski 2016).

The potential *financial* implications for consumers relate to how IoT-collected data are being used by commercial actors in the market. A main point is that consumers will be “rewarded” for good/loyal/healthy behaviour, while being “punished” for bad/disloyal/risky behaviour through **personal price discrimination** or **real-time marketing** mechanisms. In terms of trends in the consumer market, the report mentions real-time personal inventory management, interactive advertisements, customer tracking, customer profiling, physical “buy buttons” on products, and automatic checkout.

However, at present, most (Australian) consumers are not aware of the existence or concept of IoT. Still, research show that Australian homes have 9 connected devices on average, expected to increase to 29 devices by 2029. OECD[35] predicts that OECD households will have 50 connected devices by 2022 (Vulankovski 2016, p. 27). With ever more connected things in the household, the relevant consumer issue will be **serviceability and maintenance** of **hardware and software** (updates, obsolescence, device life, battery longevity, etc.), as well as device migration and data portability issues. How to manage updates and maintenance of tens or hundreds of IoT objects in the household? How to deal with manufacturers that stop supporting software for IoT objects? And if moving or renovating connected homes; how to reconnect homes, re-synchronise devices – and how to migrate data between not only single devices but integrated IoT-ecosystems in homes? (Issues such as cost of disengagement, re-configuration for new standards, severing brand loyalty, hassle of data transfer, or deletion of personal data in home devices when moving (privacy/security) (Vulankovski 2016, p. 30).

[35] Ref: http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm , ch. 6 “Emerging issues: The Internet of Things”

The report also addresses the more *conceptual* consumer issue of **"cognitive bandwidth".** This is the consumer capacity to "mentally manage daily information input". This becomes more challenging with IoT as consumers attempt to "keep on top of all our things". Consumers have to deal with all the data/information being exchanged, as well as maintenance of devices and software. The question is raised of how long it will take for consumers to be overwhelmed by so many connected devices (Vulkanovski 2016, p. 31). The result of this increased "automation of daily life" depends on the detail of reflection invested by consumers. There is also an **environmental concern**, as billions of cheap connected things will flood the market, making device disposal and waste management challenging. Suddenly, "regular" products fitted with IoT capability are turned into "e-waste".

In terms of **privacy** (a critical issue in IoT development), the report refers to both *personal privacy and information privacy* (Vulkanovski 2016, p.50). Key aspects are; the ***scale*** of data collection by things; new ***methods*** of data collection via sensors and smart things; the ***reach*** of data collection (penetrating intimate areas of our lives); the ***nature*** of data collection (data being collected covertly, consumers being less aware or consenting); and the ***depth*** of data collection, as the collective result of the four concepts will be greater than the sum of its parts.

The report makes a reference to the *EU WP29*, releasing an "Opinion on the recent developments on the internet of things" in 2014[36], outlining ten privacy and data protection challenges of IoT. The EU Opinion defines IoT by reference to an infrastructure where billions of sensors, embedded in common everyday devices, are designed to record, process, store and transfer data – having unique identifiers that interact with other devices or systems using networking capabilities. The point is that as IoT relies on extensive data processing and on unobtrusive communication/seamless data exchange, involving a significant number of stakeholders (device manufacturers, data aggregators/brokers, application developers, social platforms, device lenders/renters, etc.), it clearly raises new and significant personal data protection and privacy/security challenges according to EU WP29. It also focuses on three relevant IoT developments (**wearable computing**, **quantified self** and **home automation [domotics]**), which are *directly interfaced to the user,* and that correspond to *devices and services that are in use*, thus actually *lending themselves to an analysis under data protection laws*[37]. There are two specific new IoT risks that are considered; the ***risk of re-identification*** (of anonymised data) and the ***insufficiency of traditional consent models*** (as data are collected covertly).

Another report, published in 2015 by the *European Parliament* (on big data/smart devices and their impact on privacy)[38], addresses the two interlinked – but also *conflicting strategies* by the EU; the promotion of a **data-driven economy** and the adoption of the revised **privacy and personal data protection** framework (GDPR[39]). As "data" are central to both developments, the issues of big data, smart devices and internet of things must be addressed together. Also, the report finds that the *opacity of many existing data processing activities* have a direct and negative impact on the rights of citizens/consumers. Hence, the development of a data-driven economy should not underestimate the challenges raised for privacy and personal data protection. Therefore, the rights of digital citizens should be a main and continued focus. With the rise of cheap sensors and mobile devices, the world is already becoming increasingly connected, and IoT will contribute massively to the generation of information feeding big data analyses. **Big data** constitutes powerful analytical and predictive tools, hence there is also a concern for risks of **biased information**, **spurious correlations** and **statistical discrimination**. With more enhanced automated decision-making and behavioural targeting being based on big data output (with less human intervention, and being less comprehensible to people), it is critical that the results of big data analytics are trustworthy, transparent and verifiable.

[36] Cf: EU WP29 Opinion 8/2014: http://www.dataprotection.ro/servlet/ViewDocument?id=1088

[37] Ibid.

[38] Cf: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf

[39] General Data Protection Regulation

A 2016 report by *Rathenau Instituut*[40] ("Beyond control: Exploratory study on the discourse in Silicon Valley about consumer privacy in the internet of things"), is based on the research theme "**hyper-connected consumer**". It addresses how key stakeholders deal with privacy, and finds that the *burden of control over personal data is primarily placed on the consumers* themselves. However, this will be a challenging perspective with IoT, as consumers increasingly lose control because many smart devices often *lack screens* that consumers can interact with. Also, the *amount of devices* makes it hard to control all data flows. The report claims that smart devices will increase the tendency of consumers being subjected to *profiling and subtle persuasion*, affecting their freedom in a negative way.

The report, being exploratory in terms of studying privacy in consumer settings, also draws a future perspective based on the notion that ***privacy is about control***. In this sense, the major concern with IoT is that *consumers will lose control over their personal data*. E.g. a household filled with tens or hundreds of connected and communicating devices, that collect a process personal data, will be too difficult for consumers to control. Even with opt-out functions, and limits on data collection and data sharing, full control seems unachievable. Stakeholders interviewed in the report believe that present solutions, like screens with push buttons, will be insufficient, but that user control also can be achieved by other means – such as **built-in privacy and user control** in IoT devices, along with **granular permission systems**, ability to **turn off data streams** and systems designed for **local storage/processing of sensitive data**[41].

At the same time, stakeholders from global tech companies implicitly looked beyond the notion of privacy being synonymous with full consumer control. Some stated that **consumers would be overwhelmed with a choice for everything** (implying that too much choice is not in the best interest of consumers). Rather, by employing a **risk-based approach to privacy**, suppliers could determine beforehand types of sensitive data (and the use of these), and on the basis of this provide consumers with meaningful control. In a sense the main conclusion is that *consumers are neither able nor willing to assess risks of data collection and use* (in IoT environments) and that manufacturers of IoT-devices rather should be responsible for "performing complicated risk assessments of certain types of data collection and data use, incentivised by liability and consumer protection law"[42]. Still, it was acknowledged that "even if all data protection requirements are met, a permanent data archive combined with predictive capabilities can still be highly privacy invasive". E.g. a smart TV used as a controller for an IoT-hub of smart household devices will not only affect the individual user but all household members. Hence, even with high attention to privacy among suppliers/manufacturers, policy-makers and partly consumers, the report states that the **broader concepts of privacy remain underexposed in IoT development**.

Looking at other sources than reports and stakeholder/policy documents, Jeremy Rifkin – in his book "*Zero marginal cost society. The internet of things, the collaborative commons, and the eclipse of capitalism*" – paints an intense picture of **IoT as the "first smart-infrastructure revolution in history"** (Rifkin 2014, p.73). He anticipates the connection of every machine, business, residence and vehicle in an intelligent network, which will feed a continuous stream of big data to be processed with advanced analytics and predictive algorithms. Rifkin addresses the **wider privacy implications** of this development. The connection of "everyone and everything in a neural network **brings the human race out of the age of privacy** […] **and into the era of transparency**", he states. Historically, privacy has been a fundamental right, but never an inherent right, Rifkin claims. Until the modern era, people lived their lives publicly, while in the early capitalist period people began retreating behind locked doors, enjoying private life. Closed homes were further separated with rooms for various purposes/activities. Hence, he

[40] Cf: https://www.rathenau.nl/en/publication/beyond-control
[41] Cf. p.27: https://www.rathenau.nl/en/publication/beyond-control
[42] Cf. p.28: https://www.rathenau.nl/en/publication/beyond-control

concludes that the enclosure and privatization of human life went hand-in-hand with the enclosure and privatisation of *the commons* (Rifkin 2014, p.75). Private life, private property, the autonomous agent, and so on, turned the right to privacy into the right to exclude. Today, pervasive and ubiquitous technology, the IoT and big data, and a globally connected world more generally, **rip away these "layers of enclosure"**. Hence, the increase of global virtual publicity, transparency and collaboration challenges the traditional notion of privacy. Rifkin thus asks; "when every human being and every "thing" is connected, what boundaries need to be established to ensure that an individual's right to privacy will be protected?" (Rifkin 2014, p. 76). Commercial actors, third party data brokers, cyber criminals, governments, the curious neighbour, are all eager to get hold of information and data about private life. This challenge of harvesting, access to, and control of personal/private information is the biggest and most complex the pervasive data-driven economy is facing.

Three recent reports from SIFO address related issues in the Norwegian context; a review of how the smartphone has affected Norwegian consumers (Storm-Mathisen 2016); a study of how Norwegian stakeholders understand the challenges and possibilities connected to commercial use of personal and consumer data (Throne-Holst & Kjørstad 2016); and a study of Norwegian children's access to internet-connected toys and technologies, parents' awareness of user data being harvested, and the marketing opportunities these technologies facilitate (Kjørstad et al. 2017).

* * *

The aim of this chapter has been to review the latest developments in the definition and understanding of the IoT phenomenon. In chapter 1.4 we discussed the engagement with RFID and IoT in the years prior to project start-up (2007-2009), getting a perspective of the relevance of RFID and the coming IoT at the time. Then, in the project period (with case study research mostly conducted in the period 2010-2014), we continued to approach the enabling technologies (RFID and similar) and the visions of IoT, based on the key understandings at that time. Then, finally, as the project now is being completed, we have here reviewed the latest developments (mostly based on 2014-2017 papers and stakeholder/policy documents), getting an impression of the present ideas/notions surrounding IoT – and how the world (and IoT as a phenomenon) has changed over the years.

3 Project accomplishments

The empirical and theoretical contributions of the *RFID in Society* project has been reported on in the previous project report (del. 1 to 3) as well as through articles, conference papers, an exhibition, presentations, media contributions and the project website. In the next sub-chapters, we will describe cooperation efforts and different types of participation by project researchers. We will also go into more detail on the various publication and dissemination efforts emanating from the project.

3.1 Partners, cooperation and participation

As a way to deal with both the aim of ***methodological and case diversity***, the project aspired to have a partner constellation that signalled diversity in terms of academic and thematic perspectives. Hence, the SIFO/IMK-UiO researcher constellation worked with several different cases (library, running event, festival, toll collection, transport ticketing, waterpark, etc.), while SNF-NHH (and the affiliated master student) worked on the enhanced ski-service. TIK-UiO (the post doc) concentrated on the apparel/clothing industry, while the TIK master student studied a tracking in the care sector. Even if the case studies were conducted separately, there were several meetings and workshops carried out were the affiliated institutions shared theoretical/methodical and practical insights and ideas on how to approach the case studies, as well as on how the diverse analytical perspectives held by the different academic institutions could supplement or enrich each other (where possible).

Furthermore, there were overlapping comparative work conducted between the *RFID in Society* project and the *NFC City* project, both in terms of comparing use cases and in terms of applying academic/methodological perspectives. This ***cross-project cooperation*** can be exemplified by e.g. the thematic/analytical comparison/contrasting of ticketing services and the comparison of positivist vs interpretivist methodologies. Additionally, the *RFID in Society* project and its researchers learnt a lot about the technical development, and ecosystem thinking, from the *NFC City* innovation project. Vice versa, the latest developments in project design, and in stakeholder issues (privacy, consumer protection, methodological experiences, etc.) was implemented in the *NFC City* pilot design.

From the early phase, project researchers regularly took part in the Norwegian initiative ***IoT Value Creation Network***[43], which was funded by *Forskningsrådet* (*The Norwegian Research Council*). The *RFID in Society* project benefitted greatly from participating in these workshops, as it brought together key stakeholders from a variety of sectors in Norway that engaged with the IoT development (research institutions, trade and industry, policymakers/government agencies, etc.) The aim of the network was "unify the IoT community in Norway" in order to create a "joint strategic vision of the Internet of Things". It aimed to create a "national technology arena and a meeting place for developing new ideas, identifying national key research challenges, and disseminating research results across sectors". Through these meetings and workshops, the research group was updated on the latest developments in IoT, in particular in the

[43] Cf. http://www.internet-of-things.no/

Norwegian context, and could discuss relevant issues/cases with other participants or in plenum.

The project also touched ground with relevant IoT activities in the EU region (under the Digital Agenda initiative). Through participation by the post-doc at TIK-UiO, the seminars regarding the ***Onlife Initiative***[44] – and the *"Onlife Manifesto*[45]*: Being Human in a Hyperconnected World"* – was particularly fruitful and relevant to the *RFID in Society* project. The Initiative aspires to bring together policy, research and industry, and create a common ground to discuss the very foundations of being human – and society – in a world of rapid technological development (were the future visions of IoT is particularly central). It states that the uptake of ICT and new technology by society radically affects the human condition, modifying our relationships to ourselves, to others and to the world. The digital transition taking place "shakes established reference frameworks, which impact the public space, politics itself, and societal expectations toward policy making". Hence, the aim of the Onlife Initiative is to explore these impacts within the policy context of the Digital Agenda for Europe. Furthermore, SIFO was in dialogue with ***LSE,*** providing input on Norwegian IoT initiatives to a current study for the ***OECD Consumer Policy Committee*** on consumer aspects of the Internet of Things.

A major challenge for RFID and IoT development is standardisation. Although the project's main concern has been the potential benefits and risks associated with the development of this technology with a consumer/societal focus, SIFO was invited to be part of the RFID (or AIDC) committee at ***Standard Norge (Standards Norway).*** SIFO considered this to be fruitful for the *RFID in Society* project, as a way to gain new knowledge on the latest developments in RFID/IoT standardisation, to get in touch with relevant stakeholders participating in the committee, and to influence the standardisation efforts carried out nationally and globally with own expertise. SIFO participated in the committee – ***SN/K 178 Automatisk identifikasjon og datafangst***[46]. Other participants included; CapGemini, Datatilsynet, DNV, Dyreidentitet, GS1, HRAFN, NorSIS, OLF, Posten Norge, SAS Institute, SINTEF IKT, Telenor Objects, and others.

The committee was revived in 2010 and functioned as a mirror committee for standardisation project in ***CEN/TC 225 Automatic Identification and Data Capture (AIDC) Technologies and Applications*** and in ***ISO/JTC 1/SC 31 Automatic identification and data capture techniques***. The main mandate was to ensure that Norwegian interests were considered in the international work on RFID, and to address the relationship with other wireless and sensor technologies. Another goal was to follow up the standardisation efforts regarding global unique identificators and the coming Internet of things. From early on, there was a heavy industry focus in the committee, but over time Standards Norway sought to *increase the consumer focus in RFID/IoT development.* This was reflected in the selection of committee members. Even with high interest among committee members, and increasing relevance for society, the committee was discontinued (2014) due to lacking financial support.

Still, SIFO continued the work with international standardisation work, holding a national expert position in ***ISO/COPOLCO/WG5: Consumer protection in the global market place***, where a key priority area has been ***Privacy by design of consumer goods and services***. This is a highly relevant topic to be considered in the development of *smart consumer things and the IoT more generally.* In particular, the ISO/COPOLCO 37th Plenary[47] in Geneva (2015) was enriching, where SIFO participated in various plenary sessions and workshops on "The connected consumer in 2020 – Empowerment through standards". The main discussions centred on whether international standards can help protect consumers on the internet with regards to

[44] The Onlife Initiative: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Concept_Reengineering_Background_Paper_04112012.pdf

[45] The Onlife Manifesto: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/feb8programme.pdf

[46] Cf: https://www.standard.no/standardisering/komiteer/sn/snk-178/

[47] Cf: https://wordpress.com/page/rfidsociety.wordpress.com/19

data privacy, innovative business practices, and business-to-consumer relationships in the era of the Internet of Things.

In addition, several meetings and workshops were held with actors that the project identified to be relevant to the unfolding RFID/IoT development. Early discussions were held with ***Norsk Regnesentral*** *(Norwegian Computing Center)* on the issues of privacy and identity management. Workshops were also held with ***Datatilsynet*** *(The Norwegian Data Protection Authority)****.*** A range of applications were discussed, in particular in the transportation sector, and a wide array of potential privacy and "function creep" issues were discussed. The project group also had meetings with ***GS1 Norway*** and got to see a demonstration of RFID in distribution at the ***GS1 Norway Smart Centre***[48]. Furthermore, the project initiated several more academically oriented workshops, i.e. on theoretical-methodological issues (ANT, risk/trust, etc.), that involved other participants (e.g. from UiO). Furthermore, the project was contacted by ***commercial actors*** that intended to employ RFID in their operations, and therefore wanted to hear about the latest developments in the Norwegian context before making final decisions. These requests and ensuing discussions were fruitful for the project in terms of getting insights into market considerations and preparedness.

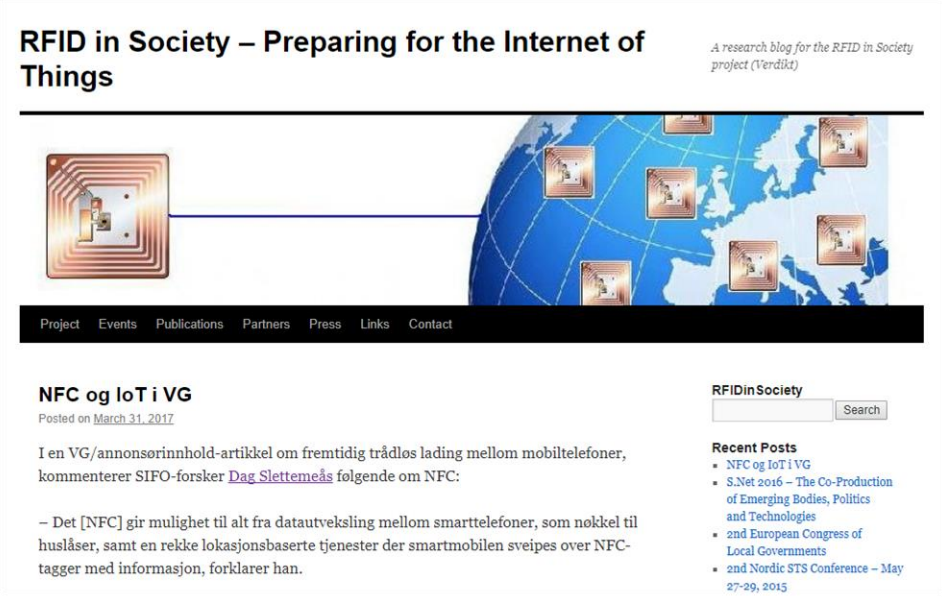
As a way to stay updated on developments (in addition to the above-mentioned activities) on the international RFID scene, and to get inspiration for cases to study and issues to address, the project researchers consulted various newsletters on a regular basis, such as; *RFID Journal*, *RFID Solutions Online*, *Retail Solutions*, *Readwriteweb* (now *Readwrite*), *ContactlessNews* (now *SecureIDnews*), and the *RFIDnews*. Key online resources were also consulted on a regular basis, such as; *Internet of Things – Europe* (http://www.theinternetofthings.eu/), *European Research Cluster on the Internet of Things (IERC)* (http://www.internet-of-things-research.eu/), *The Internet of Things Value Creation Network – Norway* (http://www.internet-of-things.no/), *EU Digital Agenda – Internet of Things* (https://ec.europa.eu/digital-agenda/en/internet-Things), and *The EC Alliance for Internet of Things Innovation (AIOTI)* (https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti).

3.2 Publications, presentations and dissemination

As a way to both inform project partners and the public about the *RFID in Society* project, a ***project website***, based on the Wordpress.com template, was launched in November 2010[49]. A blog structure was considered the best solution for easy publishing of posts on project activity. In this way it was project activities could be followed, using "dynamic" posts, in addition "static" information pages (such as Project, Events, Publications, Partners, Press, Links, Contact). After project end, the research blog will not be closed, but continue to be a source of information.

[48] Cf: http://www.gs1.no/produkter-og-tjenester/gs1-norway-smart-centre

[49] Cf: https://rfidsociety.wordpress.com/


RFID in Society – Preparing for the Internet of Things

A research blog for the RFID in Society project (Verdikt)

NFC og IoT i VG

Posted on March 31, 2017

I en VG/annonsørinnhold-artikkel om fremtidig trådløs lading mellom mobiltelefoner, kommenterer SIFO-forsker Dag Slettemeås følgende om NFC:

– Det [NFC] gir mulighet til alt fra datautveksling mellom smarttelefoner, som nøkkel til huslåser, samt en rekke lokasjonsbaserte tjenester der smartmobilen sveipes over NFC-tagger med informasjon, forklarer han.

RFIDinSociety

Recent Posts

- NFC og IoT i VG
- S.Net 2016 – The Co-Production of Emerging Bodies, Politics and Technologies
- 2nd European Congress of Local Governments
- 2nd Nordic STS Conference – May 27-29, 2015

Figure 2: Screenshot from RFID in Society research blog (Sept. 2017).

In terms of ***presenting the project and disseminating information*** about a consumer/society-centred perspective on RFID-/IoT-development, project researchers were active in a range of settings. Several internal presentations and workshops were held at the research partner institutes, to inform other researchers, and management, of the theme and project. The TIK *post doc* researcher held a TIK seminar called *"Code Walking in Paris"* on RFID in apparel, asking "can the clothes you wear become as interactive as your Facebook account? What are the realities and what are the visions of an emerging Internet of Things?"[50]. Also, a two hour lecture was given (by SIFO) to MA-students at ***TIK, University of Oslo (UiO)*** on the topic "RFID – the small technology with the big potential - and challenges"[51]. Presentations were furthermore given by SIFO researchers to the ***Norwegian Consumer Council***, as well to the ***Department of Private Law, UiO***[52] - on the topic *RFID/IoT, data harvesting and privacy*. In addition, SIFO was invited by ***DSB (Norwegian Directorate for Civil Protection)*** – along with other tech-experts from IBM, Telenor, Teknologirådet, Sintef, NTNU, FFI, etc. – to present technology-related opportunities and risks in a long-term perspective (2040). The SIFO-presentation introduced the importance of a consumer perspective on tech development, specifically addressing 1) *smart products*, 2) *contactless technology*, and 3) *Internet of Things*[53].

Internationally, SIFO was invited panelist to the ***The Economic Forum / European Congress of Local Governments***[54], on the "The role of metropolises in nurturing innovations"[55]. SIFO used examples from innovation collaborations in Norway and abroad (RFID/NFC, IoT, smart cities – based on experiences from both the *RFID in Society* and the *NFC City* projects), in the panel discussions with French, Polish, Latvian and Ukrainian panelists. Here, SIFO signalled to the Eastern European research community – and local governments – the role of IoT as part of the future for social innovation in European metropolises[56].

In addition to the public dissemination activities mentioned above, bringing the general theme of IoT, as well as the specifics of the *RFID in Society* project to the wider academic/policy

[50] Cf: https://rfidsociety.wordpress.com/2012/08/29/new-tik-seminar-code-walking-in-paris/
[51] Cf: https://rfidsociety.wordpress.com/2010/12/14/ma-lecture-on-rfid-at-tik-university-of-oslo/
[52] Cf:http://www.jus.uio.no/ifp/om/organisasjon/seri/arrangementer/2014/tirsdagskaffeseminar/11%3A-3.-juni%3A-rfid-in-society/
[53] Cf: https://rfidsociety.wordpress.com/2015/05/19/foredrag-dsb-risiko-2040/
[54] Cf: http://www.forum-ekonomiczne.pl/?lang=en
[55] Ref: http://www.forum-ekonomiczne.pl/2nd-european-congress-of-local-governments/?lang=en#.WVN8WuvyiM9
[56] Cf: https://rfidsociety.wordpress.com/2016/04/08/european-congress-of-local-goverments/

audience, TIK created a ***two-day interactive RFID exhibition*** at ***"Forskningsdagene"*** (2012). The general public was invited to experience the booming net-based society, where information, physical objects and people are connected to the internet[57]. The exhibition was a huge success. At the TIK stand – or "TIK boutique" – the audience could choose various garments and pass by a range of RFID antennas. The garments were registered and messages were sent to Twitter, indicating the *location and story behind the product*. At the end of the process, information could be read at the Twitter account "TIK_butikk". The garments were eventually "sold" at the checkout point, and "customers" were given a receipt (however, the product could [unfortunately] not be taken home). The stand was particularly popular among children and youth, and they were guided by TIK master students that engaged in conversations about advantages and disadvantages relating to IoT[58].

In terms of written efforts, project researchers have been active in several academic outlets[59]. Papers have been presented at various conferences; TIK-UiO has i.e. presented at the ***8th Annual Meeting of the Society for the Study of New and Emerging Technologies (S.Net)*** in Bergen, Norway ("Shopping is human nature: RFID, privacy and the omni-channel customer", 2016), and at the ***2nd Nordic STS Conference*** in Copenhagen, Denmark ("Enough of Ethnography? Or: What I learned from being an ad-hoc lab rat in an Internet of Things", 2015). SIFO presented several papers internationally, i.e. at ***ESA Consumption Research Network Midterm Conference*** in Porto, Portugal ("Internet of things – RFID in consumers' everyday life", 2014), and at the ***EuroCPR conference – Prospects, Challenges and Limits to User-Centric Approaches in the Digital Information Society***, in Brussels, Belgium ("Public/user reception of RFID enabled toll/ticketing applications – experiences from the implementation of AutoPASS and Ruter in Norway", 2014).

Regarding manuscripts for peer-reviewed journals and books, several have been published already, while some are still in the process of being submitted or resubmitted to new journals. There have also been efforts to create cross-project synergies, between *RFID in Society* and *NFC City* through co-authorship.

In terms of accepted or published material, the latest manuscript accepted is a book chapter in ***Markedsføring og forbrukerinteresser i det 21. århundret – samfunnsvitenskapelige perspektiver*** ("Big Data og Tingenes Internett – om den «oppkoplede forbruker» og nye markedsføringsrelasjoner", 2018). Furthermore, articles have been published in ***Information Systems Frontiers*** ("Consumer adoption of RFID-enabled services. Applying an extended UTAUT model", 2016), and in ***Info*** ("RFID in toll/ticketing – a user centric approach", 2014). In addition ***two master theses*** have been successfully submitted, accepted and published; 1) "Å skape en mulig omsorgsteknologi. En studie av et møte mellom sporingsteknologi og et nytt bruksområde» (UiO, 2012), and 2) "Intention to use RFID-enabled services: theoretical review and case study" (NHH, 2012). Four project reports have also been published (including this one); 1) "RFID in Society – preparing for the internet of things. Case Criteria & Selection" (SIFO, 2017), 2) "RFID in Society – preparing for the internet of things. Case Analyses & Evaluation" (SIFO, 2017), 3) "RFID in Society – preparing for the internet of things. Handbook of Methods" (SIFO, 2017), and 4) "RFID in Society – preparing for the internet of things. Final Report & Summary" (SIFO, 2017).

In addition several manuscripts have been through review processes and are in the process of being submitted/resubmitted to peer-reviewed journals, such as; 1) "Bodies matter: Counting with RFID in Norwegian apparel" (TIK), 2) "Glonique bodies in RFID. Corporate practices between inventory accuracy and omnichannel shopping" (TIK), 3) "Developing an appropriation framework for Internet of Things (IoT) ecosystem research and innovation"

[57] Cf: https://rfidsociety.wordpress.com/2012/08/29/forskningsdagene-i-oslo-velkommen-til-samfunnett/
[58] Cf: https://rfidsociety.wordpress.com/2012/09/27/forskningsdagene-a-successful-event/
[59] See project blog for full reference. https://rfidsociety.wordpress.com/publications/

(SIFO/Telenor), and 4) ”From smartcard to smartphone: A user perspective on transport ticketing.” (SIFO/Telenor).

Finally there has been some ***mass media contributions***, such as in **VG** (annonsørinnhold: “Snart vil du kunne ‘stjele’ mobilbatteri fra venner”)[60], in **Vårt Land** (“- Selvsagt har vi noe å skjule; vårt eget privatliv”)[61], in **Klassekampen** (“Smart-tingene”)[62], in **Computerworld** (“Veien til makten”)[63] and (“Deler ut 204 millioner til it-forskning”)[64], in **Forskningsdagene.no** (Forskningsdagene: “Velkommen til SamfunNETT!”)[65], and in **SV-fakultetet/sv.uio.no** (“TIK merker klær”)[66], (“Full pott på forskningstorget”)[67], and (“Hva gjør du nå, Stefanie Jenssen?”)[68].

[60] http://vg.no/annonsorinnhold/smart/komplett/268-snart-vil-du-kunne-stjele-mobilbatteri-fra-venner

[61] http://www.vl.no/nyhet/selvsagt-har-vi-noe-a-skjule-vart-eget-privatliv-1.790134

[62] http://www.klassekampen.no/61708/article/item/null/smarttingene

[63] http://www.idg.no/computerworld/article265251.ece

[64] http://www.idg.no/computerworld/article166817.ece

[65] http://arrangor.forskningsdagene.no/torgarrangement/vis.html?tid=637450

[66] http://www.sv.uio.no/for-ansatte/aktuelt/aktuelle-saker/2012/bygginga-i-ganghtml

[67] http://www.sv.uio.no/psi/forskning/grupper/ekup/aktuelle-saker/2012/arrangementstotte-forskningstorget.html

[68] http://www.sv.uio.no/for-ansatte/aktuelt/hva-gjor-du-naa/hva-gjor-du-na-stefanie-jensen-18-04.12.html

4 Summary and conclusion

The *RFID in Society* project (full project name: *RFID in Society – Preparing for the Internet of Things. Researching Opportunities and Obstacles in RFID innovation)* has truly been a knowledge-building project. The project received funding from the VERDIKT-programme as a "researcher project" (*forskerprosjekt*), and commenced in 2010. The aim was to study how novel technologies (such as RFID) and emerging paradigms (such as IoT) would affect individuals/consumers and community/society. This implied a focus on "people-centric" applications, addressing both opportunities and challenges when such technology enter everyday life.

The backdrop was rapid growth in applications for RFID and sensor technology, and the emerging vision/paradigm of a future *Internet of things* (IoT). In the period around 2010, IoT had only recently become a central theme in European and Norwegian ICT research and politics, while RFID and other enabling technologies were considered key enablers for a global IoT system. IoT was still "visionary" and elusive at the time, while RFID was "tangible" with a range of implemented RFID-applications/services.

The project has, through a cross-disciplinary approach (although with more focus on social science perspectives than technical perspectives and design), explored a range of different cases, methodologies, and methods of analysis – all with the aim of providing a better understanding of the RFID/IoT phenomenon and its potential future position in society. The outcome of the research can inform Norwegian research/innovation efforts as well as policy/organised interests when manoeuvring in the RFID/IoT field.

Being a knowledge-building project, it is the totality of the research efforts of the *RFID in Society* project that has been in focus (sketched below):

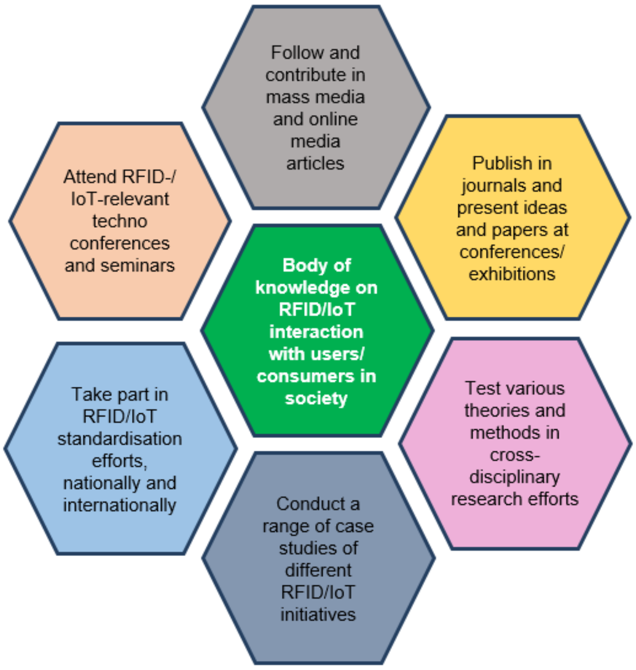

Follow and contribute in mass media and online media articles
Attend RFID-/ IoT-relevant techno conferences and seminars
Publish in journals and present ideas and papers at conferences/ exhibitions
Body of knowledge on RFID/IoT interaction with users/ consumers in society
Take part in RFID/IoT standardisation efforts, nationally and internationally
Test various theories and methods in cross-disciplinary research efforts
Conduct a range of case studies of different RFID/IoT initiatives

Figure 3: Body of knowledge generated from the *RFID in Society* research efforts

Most of the practical research was carried out in the period 2010-2014/2015, although the project continued until 2017, due to unforeseen circumstance at two of the research institutions. From the project initiation until present day, we see that the discourse around IoT has changed. Starting from a very industry-focussed "ICT" domain, with RFID being the prime figure and key enabler for a future Internet of things, we have seen a dramatic reorientation towards consumer and societal application areas. With this has come the dwindling role of RFID (at least in consumer-related application areas) at the expense of a wide array of technologies that make things and environments "smart", "intelligent" and "connected".

In terms of applications aimed at the consumer-citizen, we see a particular dramatic surge in smart consumer products, smart electronics, connected cars, wearables/smart health applications, smart homes, smart advertising – where most things now can be fitted with chips and means of communications. Hence, the primary tech-consumer domain in the early phase – RFID in retail – has somewhat lost momentum (at least at the consumer end), while smart products have pushed forward (somewhat skipping retail, and enabling a more direct producer-consumer engagement). Now, the key enabler (for consumers) is the smartphone, with a range of communication capabilities towards smart environments (using Wi-Fi, Bluetooth, NFC, apps, embedded sensors, etc.)

Both the technological and the cultural premises have thus changed over the years, with consumers becoming considerably more *active in "building" the IoT* through direct participation (and consequent data generation) via their smartphones and smart-things – feeding the IoT with an exponential data stream. A major part of the potential for value-creation is identified in this IoT/Big Data symbiosis.

Still, even with consumers engaging more vividly with IoT-type services and applications, research finds that *consumer awareness* is still low regarding the concept itself. A recent report from SIFO, commissioned by the ministry[69], surveys IoT awareness and engagement in the Norwegian population (Kjørstad et al. 2017). The study finds that 22% of consumers have

[69] Barne- og likestillingsdepartementet

heard about the concept "IoT" through mass media or other media channels, with 33% for men and 10% for women. In terms of age, there is falling awareness with increasing age; 25% of those between 18-25 years have heard of IoT, but only 14% among those between 60-80 years. Actual adoption of net-connected things is also surveyed, with examples such as connected consumer products (toys, fridges, video surveillance, etc.), robots (lawn mowers, vacuum cleaners), smart home solutions, connected cars, wearables, chipped pets, and so on. The list of 22 exemplified items show that 68% of consumers and their households have one or more net-connected "things" at home, while only 32% have no practical experience with IoT at home (that they are aware of).

Even with more things becoming connected (as stated in the 2017 Ofcom report[70]), many IoT products and innovations still lack a *clear and communicable consumer benefit* that will take IoT into the "next phase", at least at the consumer level. Both the 2017 reports from SIFO and Ofcom indicate that public awareness is low, even though mass media and stakeholders tend to state the opposite – that IoT is already changing society drastically. We are still at a stage where IoT is more prevalent on the "discursive level" than on the "tangible-things" level.

Even if IoT is immature, in particular at the consumer level, there is much activity on the more collective/big scale application areas, where most things are becoming gradually "smarter". This is exemplified by the Norwegian IoT value-creation network[71], where IoT is identified as; smart cities, smart transportation, smart energy, smart industry, smart buildings, smart health and smart living. The key challenge for the evolution of IoT is the trade-off situation between the technology's inherent *grand risks vs grand opportunities*, i.e. referred to by the 2015 EU report[72] as the *two interlinked but conflicting strategies of simultaneously promoting a data-driven economy as well as a stricter privacy and personal data protection framework*. This "technology paradox" (cf. Mick and Fournier 1998, Kozinets 2008, Feenberg 2010) associated with IoT is still not solved, and will continue to boggle the minds of innovators and politicians in the years to come.

* * *

In this landscape of a global technological disruption and pervasive technology development – affecting the whole of society – the *RFID in Society* project is merely one building block in terms of getting to grips with, and seeking to understand the impact of, the evolving Internet of things.

[70] 2017 Ofcom report: https://www.ofcom.org.uk/__data/assets/pdf_file/0007/102004/Review-of-latest-developments-in-the-Internet-of-Things.pdf
[71] Cf: http://www.internet-of-things.no/
[72] Cf: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf

References

Atzori, L., Ilera, A., & G. Morabito (2010). "The Internet of Things: A Survey". *Computer Networks, 54*, 2787-2805.

Bjørnhaug, A. S. (2012). *Å skape en mulig omsorgsteknologi. En studie av et møte mellom sporingsteknologi og et nytt bruksområde*. Master thesis, TIK, University of Oslo.

CI (Consumers International) (2016). *Connection and protection in the digital age. The Internet of things and challenges for consumer protection.* Consumers International, April 2016. Ref: http://www.consumersinternational.org/media/1292/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf

Feenberg, A. (2010). "Ten paradoxes of technology". *Techné, 14*(1), 3-15

Fotland, Astri Irene (2012). *Intention to use RFID-enabled services : theoretical review and case study*. Master thesis, NHH.

Helle-Valle, J. (2014). «Internet of Things, datahøsting og personvern». Presentation held at Institutt for privatrett, University of Oslo, June 3, 2014.
Ref: http://www.jus.uio.no/ifp/om/organisasjon/seri/arrangementer/2014/tirsdagskaffeseminar/11%3A-3.-juni%3A-rfid-in-society/

Helle-Valle, J. (2014). "RFID, IoT, datahøsting og personvern". Presentation held at Forbrukerrådet, Oslo, August 20, 2014.

Jenssen, S. R. (2016). "Shopping is human nature: RFID, privacy and the omni-channel customer". Paper presented at the session Digital technologies in society, as part of the *The 8th Annual Meeting of the Society for the Study of New and Emerging Technologies (S.Net)*. Centre for the Study of the Sciences and the Humanities, University of Bergen, October 11-14, 2016.

Jenssen, S. R. (2015). "Enough of Ethnography? Or: What I learned from being an ad-hoc lab rat in an Internet of Things". Paper presented at the *2nd Nordic STS Conference*, Copenhagen, Denmark, May 27-29, 2015.

Jenssen, S. R. (2012). "Lek, (K)lær og Loven i Tingenes Internett" – an interactive RFID test lab and exhibition (RCN-funded) for the general public at *"Forskningsdagene",* a two-day event in Oslo, Sept. 21-22, 2012.

Kjørstad, I., T. G. Rosenberg, D. A. Storm-Mathisen & D. Slettemeås (2017). *Barn og internettkoblede leker og teknologier – IoT*. SIFO Oppdragsrapport nr. 8-2017. Ref: http://www.hioa.no/Om-HiOA/Senter-for-velferds-og-arbeidslivsforskning/SIFO/Publikasjoner-fra-SIFO/Barn-og-internettkoblede-leker-og-teknologier-IoT

Kozinets, R. V. (2008). "Technology/Ideology: How Ideological Fields Influence Consumers' Technology Narratives". *Journal of Consumer Research, 34*(6), 865-881

Nysveen, H. & P. E. Pedersen (2016). "Consumer adoption of RFID-enabled services. Applying an extended UTAUT model". *Information Systems Frontiers, 18* (2), 293–314

Rifkin, J. (2014). *The zero marginal cost society. The internet of things, the collaborative commons, and the eclipse of capitalism.* New York: Palgrave Macmillan.

Slettemeås, D. (2007a). «RFID – the 'next step' in consumer-product relations or Orwellian nightmare?» Presentation held at the *Nordic Consumer Policy and Research Conference*, Helsinki, October 3-5, 2007.
Ref: http://www.hioa.no/extension/hioa/design/hioa/images/sifo/files/file72319_helsinki-rfid-pres031007.pdf

Slettemeås, D. (2007b). *Forbrukernes stilling i informasjonssamfunnet*. SIFO oppdragsrapport nr. 15, 2007. Oslo: SIFO.
Ref: http://www.hioa.no/extension/hioa/design/hioa/images/sifo/files/file72356_oppdragsrapport2007-15web.pdf

Slettemeås, D. (2009). «RFID – the 'Next Step' in Consumer-Product Relations or Orwellian Nightmare? Challenges for Research and Policy». *Journal of Consumer Policy, Vol. 32, Iss. 3*, pp. 219-244.
Ref: https://link.springer.com/article/10.1007%2Fs10603-009-9103-z

Slettemeås, D. (2010). «RFID: den lille teknologien med det store potensialet – og de store utfordringene». Lecture given to MA-students at TIK, University of Oslo, December 7, 2010.
Ref: http://www.hioa.no/extension/hioa/design/hioa/images/sifo/files/file77309_tik-rfidforelesning-071210-ds-final.pdf

Slettemeås, D. (2015) «RISIKO 2040 – Teknologiske drivkrefter i fremtidens Norge». Presentation held at DSB, Tønsberg, January 29, 2015.
Ref: http://www.hioa.no/extension/hioa/design/hioa/images/sifo/files/file79998_risiko2040-dsb-dagsifo-290115-ver2.pdf

Slettemeås, D. (2016) «The role of metropolises in nurturing innovations». Invited panelist at the *2nd European Congress of Local Goverments*, Krakow, Poland, April 5-6, 2016.
Ref: http://www.forum-ekonomiczne.pl/2nd-european-congress-of-local-governments/?lang=en#.VwdyjU1f05s

Slettemeås, D., A. Storm-Mathisen & J. Helle-Valle (2017). RFID in Society – preparing for the internet of things. Case Criteria & Selection. SIFO professional report nr. 2, 2017. Oslo: SIFO.

Slettemeås, D., A. Storm-Mathisen & J. Helle-Valle (2017). *RFID in Society – preparing for the internet of things. Case Analyses & Evaluation.* SIFO professional report nr. 3, 2017. Oslo: SIFO.

Slettemeås, D., A. Storm-Mathisen & J. Helle-Valle (2017). *RFID in Society – preparing for the internet of things. Handbook of Methods.* SIFO professional report nr. 4, 2017. Oslo: SIFO.

Slettemeås, D. (2018). "Big Data og Tingenes Internett – om den «oppkoplede forbruker» og nye markedsføringsrelasjoner". Accepted chapter 7 in the book *Markedsføring og forbrukerinteresser i det 21. århundret – samfunnsvitenskapelige perspektiver*. Oslo: Universitetsforlaget.

Storm-Mathisen, A. (2014). "RFID in toll/ticketing – a user centric approach". *Info, 16* (6), 60-73.

Storm-Mathisen, A. (2016). *Forbrukere og smarttelefon – nye muligheter og utfordringer, en kunnskapsgjennomgang*. Oppdragsrapport nr. 15 – 2016. Oslo: SIFO. Ref: http://www.hioa.no/Om-HiOA/Senter-for-velferds-og-arbeidslivsforskning/SIFO/Publikasjoner-fra-SIFO/Forbrukere-og-smarttelefon

Storm-Mathisen, A. & J. Helle-Valle (2014). "Internet of things – RFID in consumers' everyday life". Paper presented at *ESA Consumption Research Network Midterm Conference*, University of Porto, Portugal, September 3-6, 2014.

Storm-Mathisen, A. & J. Helle-Valle (2014). "Public/user reception of RFID enabled toll/ticketing applications – experiences from the implementation of AutoPASS and Ruter in Norway". Paper in proceedings from the *EuroCPR conference 2014 – Prospects, Challenges and Limits to User-Centric Approaches in the Digital Information Society*. Session 2B – Case Studies on Consumption Practices. The Centre for European Policy Studies (CEPS), Brussels, March 24-25, 2014.

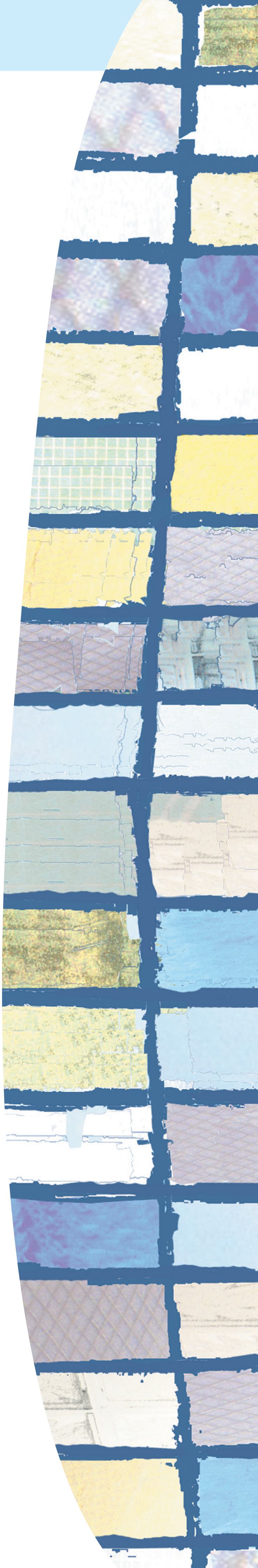
Throne-Holst, H. & Kjørstad, I. (2016). *Hva koster gratis? Kommersiell bruk av personopplysninger og forbrukerdata*. Oppdragsrapport 11- 2016. Oslo: SIFO.

Vulkanovski, A. (2016). *"Home, Tweet Home": Implications of the Connected Home, Human and Habitat on Australian Consumers*. Sydney: Australian Communications Consumer Action Network. Ref: https://accan.org.au/files/Reports/HomeTweetHome_IoT_Report-v2.pdf

Consumption Research Norway SIFO at Oslo and Akershus University College of Applied Sciences (HiOA) has a special responsibility to contribute to the knowledge base for consumer policy in Norway and will develop new knowledge about consumption, consumer policy and consumer position and role in society.

Key research topics are:

- consumers in the market and consumer choice
- household resource allocations
- consumer economy - debt development and poverty
- technological development and consumers' every day life
- digital daily life and coping
- environmental effects of different types of consumption
- food and eating habits
- textiles - value chains - consequences for everyday life and environment
- consumption significance for social inclusion
- consumer policy



SIFO
Consumption Research Norway
OSLO AND AKERSHUS
UNIVERSITY COLLEGE
OF APPLIED SCIENCES

Oslo and Akershus University college
of Applied Sciences
Consumption Research Norway
PO box 4 - St. Olavs plass - NO-0130 Oslo.
Visiting adress: Stensberggt. 26, Oslo.
Phone: +47 67 23 50 00
E-mail: post@hioa.no **Internet:** www.hioa.no/sifo