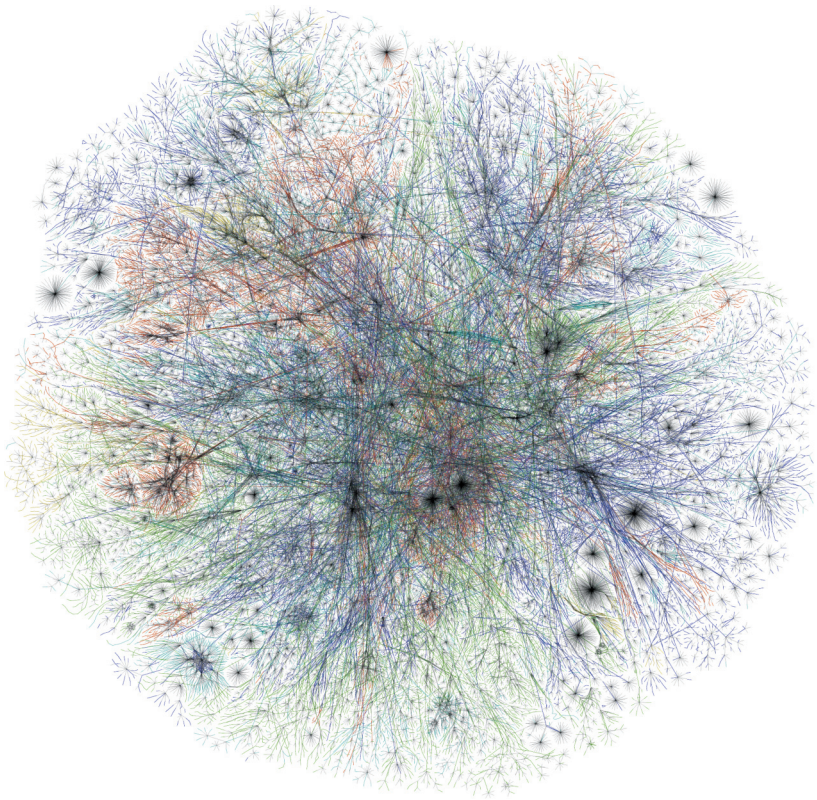
Åbo Akademi University

Magnus Westerlund

A Study of EU Data Protection Regulation and Appropriate Security for Digital Services and Platforms



Magnus Westerlund

Degrees and studies

BSc in Electrical Engineering, Information Technology,
Arcada University of Applied Sciencies, Finland

MSc in International Management,
University of Reading, United Kingdom

Pedagogical Certificate
Åbo Akademi University, Finland

DSc (BA), Information Systems
Åbo Akademi University, Finland

Portrait photo: Mikael Karmano

Åbo Akademi University Press
Tavastgatan 13, FI-20500 Åbo, Finland
Tel. +358 (0)2 215 3478
E-mail: forlaget@abo.fi

A study of EU data protection regulation and appropriate security for digital services and platforms

Magnus Westerlund

Information Systems
Faculty of Social Sciences, Business and Economics
Åbo Akademi University
Åbo, Finland, 2018

Supervisors

Doc. Markku Heikkilä
Åbo Akademi University
Faculty of Social Sciences, Business and Economics
Information Systems
Fänriksgatan 3 A 507
20500 Åbo
Finland

Prof. emeritus Christer Carlsson
Institute for Advanced Management Systems Research
Auriga Business Center
20100 Turku
Finland

Dr. Joachim Enkvist
Åbo Akademi University
Faculty of Social Sciences, Business and Economics
Commercial Law
Gezeliusgatan 2
20500 Åbo
Finland

Reviewers

Prof. emerita Louise Yngström Valdre
Department of Computer and Systems Sciences
Stockholm University
Sweden

Prof. Juha Lavapuro
Faculty of Law
University of Turku
Finland

Opponent

Prof. emerita Louise Yngström Valdre
Department of Computer and Systems Sciences
Stockholm University
Sweden

ISBN 978-952-12-3693-8
ISBN 978-952-12-3694-5 (PDF)
Painosalama Oy – Turku, Finland 2018

Abstract

A law often has more than one purpose, more than one intention, and more than one interpretation. A meticulously formulated and context agnostic law text will still, when faced with a field propelled by intense innovation, eventually become obsolete. The European Data Protection Directive is a good example of such legislation. It may be argued that the technological modifications brought on by the EU General Data Protection Regulation (GDPR) are nominal in comparison to the previous Directive, but from a business perspective the changes are significant and important. The Directive's lack of direct economic incentive for companies to protect personal data has changed with the Regulation, as companies may now have to pay severe fines for violating the legislation.

The objective of the thesis is to establish the notion of trust as a key design goal for information systems handling personal data. This includes interpreting the EU legislation on data protection and using the interpretation as a foundation for further investigation. This interpretation is connected to the areas of analytics, security, and privacy concerns for intelligent service development. Finally, the centralised platform business model and its challenges is examined, and three main resolution themes for regulating platform privacy are proposed. The aims of the proposed resolutions are to create a more trustful relationship between providers and data subjects, while also improving the conditions for competition and thus providing data subjects with service alternatives.

The thesis contributes new insights into the evolving privacy practices in the digital society at an important time of transition from the service driven business models to the platform business models. Firstly, privacy-related regulation and state of the art analytics development are examined to understand their implications for intelligent services that are based on automated processing and profiling. The ability to choose between providers of intelligent services is identified as the core challenge. Secondly, the thesis examines what is meant by appropriate security for systems that handle personal data, something the GDPR requires that organisations use without however specifying what can be considered appropriate. We propose a method for active network security in web software that is developed through the use of analytics for detection and by inserting data generators into a software installation. The active network security method is proposed as a framework for achieving compliance with the GDPR requirements for services and platforms to use appropriate security. Thirdly, the platform business model is considered from the privacy point of view and the implication of "processing silos" for intelligent services. The centralised platform model is considered problematic from both the data subject and from the competition standpoint. A resolution is offered for enabling user-initiated open data flow to counter the centralised "processing silos", and thereby to facilitate the introduction of decentralised platforms.

The thesis provides an interdisciplinary analysis considering the legal study (lex lata) and additionally the resolution (lex ferenda) is defined through argumentativist legal dogmatics and (de lege ferenda) of how the legal framework ought to be adapted to fit the described environment. User-friendly Legal Science is applied as a theory framework to provide a holistic approach to answering the research questions. The User-friendly Legal Science theory has its roots in design science and offers a way towards achieving interdisciplinary research in the fields of information systems and legal science.

Helsinki, 25.03.2018

Magnus Westerlund

Sammandrag

En lag har ofta mer än ett syfte, mer än en avsikt och mer än en tolkning. En noggrant formulerad och sammanhangsagnostisk lagtext kommer fortfarande att bli föråldrad när den står inför ett område som pådrivs av intensiv innovation. Det europeiska dataskyddsdirektivet är ett bra exempel på en sådan lagstiftning. Man kan hävda att de tekniska förändringar vilka medförs av den nyintroducerade allmänna dataskyddsförordningen i EU (GDPR) är nominella i jämförelse med det tidigare direktivet, men ur ett affärsperspektiv är förändringarna betydande och viktiga. Direktivets brist på direkta ekonomiska incitament för företag att skydda personuppgifter har ändrats genom att förordningen träder i kraft, eftersom företag nu måste betala markanta böter om de finnes skyldiga till att ha brutit mot lagstiftningen.

Syftet med avhandlingen är att etablera begreppet förtroende som ett viktigt designmål för informationssystem som hanterar personuppgifter. Detta innefattar att tolka EU: s lagstiftning om dataskydd och att använda tolkningen som en grund för vidare utredning. Denna tolkning kopplas till områdena analytik, säkerhet och integritetsfrågor för utveckling av intelligenta tjänster. Slutligen undersöks den centraliserade plattformsmodellen och dess utmaningar, för att ge tre förslag för dataskyddsreglering av plattformar. Syftet med de föreslagna förändringarna är att skapa ett mer tillförlitligt förhållande mellan leverantörer och registrerade, samtidigt som man förbättrar konkurrensvillkoren och därigenom tillhandahåller de registrerade med tjänstealternativ.

Avhandlingen bidrar med nya insikter om förändrad integritetspraxis i det digitala samhället, vid en viktig övergångstid från servicedrivna affärsmodeller till plattformmodeller. Först undersöks integritetsregleringen och forskningen inom analytik för att förstå deras konsekvenser för intelligenta tjänster, vilka bygger på automatisk bearbetning och profilering av persondata. Möjligheten att välja mellan leverantörer av intelligenta tjänster identifieras som kärnutmaningen. För det andra undersöks vad som avses med lämplig säkerhet för system som hanterar personuppgifter, något som GDPR kräver att organisationer använder utan att dock specificera vad som kan anses lämpligt. Vi föreslår en metod för aktiv nätverkssäkerhet i webbprogramvara som utvecklas genom att använda analytik för detektering och genom att sätta in datageneratorer i en mjukvaruinstallation. Den aktiva nätverkssäkerhetsmetoden föreslås som ett ramverk för att uppnå överensstämmelse med GDPRs krav på användningen av lämplig säkerhet i tjänster och plattformar. För det tredje utforskas affärsmodellen för plattformar ur privatlivets synvinkel och konsekvenserna av "bearbetningssilon" för intelligenta tjänster. Den centraliserade plattformsmodellen anses problematisk både ur den registrerades synvinkel och från en konkurrenssynpunkt. Ett förslag framförs för att möjliggöra användarinitierade öppna dataflöden för att motverka centraliserade

"bearbetningssilon" och därigenom underlätta lanseringen av decentraliserade plattformar.

Avhandlingen ger en tvärvetenskaplig analys som utgår från den rättsvetenskapliga studien (lex lata). De givna förslagen (lex ferenda) definieras genom en rättsdogmatisk metod och de lege ferenda om hur den rättsliga ramen bör anpassas för att passa den beskrivna miljön. User-friendly Legal Science (användarvänlig rättsvetenskap) appliceras som en teoriram för att ge en helhetssyn i sökandet av svar på forskningsfrågorna. Den användarvänliga rättsvetenskapen har sina rötter i designvetenskap och erbjuder ett sätt att uppnå tvärvetenskaplig forskning inom informationssystem och rättsvetenskap.

Helsingfors, 25.03.2018

Magnus Westerlund

Acknowledgements

Writing this doctoral thesis has awarded me tremendous opportunities to meet researchers from all over the world and to learn from them. The journey has taken me to many interesting places in the physical world and into intellectual conundrums I could not have imagined beforehand. There have been more contributors and influencers to this research than I can thank here, still, you have all been important during this process that is now commemorated by this doctoral thesis.

First, I would like to thank the pre-examiners Prof. emerita Louise Yngström Valdre and Prof. Juha Lavapuro for their thorough examination and corroborating feedback. Additionally, I would also like to thank Prof. emerita Louise Yngström for acting as opponent in the defence.

I have had the privilege to be supervised by Prof. emeritus Christer Carlsson. The trust he has shown in me that this process will eventually result in a fitting end, has encouraged me to let the research process take control of the direction. The work to finalise the thesis has benefitted significantly from his advice.

Dr. Joachim Enkvist has been a prominent influence in my decisions first to choose an academic career and then to start working with research. He has also been instrumental in the choice of topic and a splendid sparring partner in analysing how legislation can be interpreted in a technical setting.

Doc. Markku Heikkilä joined the process as a supervisor at a later stage and I would like thank him for his supportive comments and for helping to finalise the process. Prof. Anssi Öörni also deserves recognition for showing me the necessary freedom to continue the process to the end.

There have been several co-authors for the papers included in this thesis and I want to express gratitude to all of you. In particular, Dr. Göran Pulkkis who has been a rock throughout the process and with who I have co-written most over the years. Göran, your energy and commitment to achieving a result is always inspiring.

There has also been numerous colleagues that have influenced me positively in the research process. First I would like to highlight the role of Dr. Carl-Johan Rosenbröijer and our in-depth discussions of research and life in general. It has been an honour to sail all over the Baltic sea with you, Captain. Dr. Niklas Ericsson deserves recognition for taking the time to debate the theoretical intricacies of IS research and for highlighting opportunities connected to research. Further I would like to thank MSc Jan-Anders Ray for reviewing the language of the thesis and Dr. Jonny Karlsson for being a good friend and an encouraging research colleague.

This doctoral thesis would not have been possible without the financial support from Arcadas Stipendiefonder and Fonden för teknisk utveckling och forskning. Here I would specifically like to thank Prof. Henrik Wolff for his visionary work and for supporting research at Arcada University of Applied Sciences.

Finally, I would like to thank family and friends, in particular Piia for being helpful in numerous ways, for staying supportive and positive throughout. Thank you for being understanding when I at times have been absent both physically and intellectually.

What a journey it has been!

List of original publications

1. **Enkvist, J. and Westerlund, M. (2013). Personuppgiftsskydd – med särskild betoning på profilering, *JFT – Journal of the Law Society of Finland* (2)2013, pp. 85-113.**

2. **Westerlund, M. and Enkvist, J., (2013). Profiling Web Users – In light of the proposed EU Data Protection Regulation, *Retfaerd - Nordic Journal of Law and Justice*, Vol. 36, Nr 4/143, pp. 46-62.**

3. **Westerlund, M. and Enkvist, J. (2016). Platform privacy: the missing piece of data protection legislation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7(1)2016, pp. 2-17.**

4. **Westerlund, M. Hedlund, U., Pulkkis, G. & Björk, K-M. (2014). A Generalized Scalable Software Architecture for Analyzing Temporally Structured Big Data in the Cloud. *New Perspectives in Information Systems and Technologies*, Volume, 559, Springer.**

5. **Xiang, J., Westerlund, M., Sovilj, D., and Pulkkis, G. (2014). Using Extreme Learning Machine for Intrusion Detection in a Big Data Environment, *7th ACM Workshop on Artificial Intelligence and Security (AISec14) collocated with 21st ACM Conference on Computer and Communications (CCS14).***

6. **Paarnio, P., Stenvall, S., Westerlund, M., and Pulkkis, G. (2015). Active Intrusion Management for Web Server Software: Case WordPress, *Tenth International Multi-Conference on Computing in the Global Information Technology (ICCGI 2015).***

Table of contents

List of Tables and Figures

Part I – Thesis

I grew up with the understanding that the world I lived in was one where people enjoyed a sort of freedom to communicate with each other in privacy, without it being monitored, without it being measured, analysed or sort of judged by these shadowy figures or systems, any time they mention anything that travels across public lines.

—Edward Snowden

1. Introduction

In a world not long ago, the meaning of privacy was a relatively trivial matter. The walls of private property and personal correspondence have defined privacy. In the Western world, the right to privacy has been a fundamental right for a long time. In some countries, trespassing on another man's private property could justify, in some cases, the use of lethal force to repel the intruder. Opening letters addressed to someone else has a maximum penalty of imprisonment in many countries. Von Koskull (2002) considers that the legal concept of privacy and its notions of kin (private life, personal integrity) are linked to historically changing socio-economic conditions and these notions are related also to cultural values.

In the digital world, the word privacy has many meanings. For some, there is no difference between the physical world and the digital, while for others, privacy does not exist in a digital world, hence creating an illusion of a fully transparent environment. As the business world faces digitalisation challenges in adopting new technologies and establishing new revenue models, balancing the right to privacy for the individual consumer is likewise demanding. Many of the most financially successful online businesses employ a revenue model primarily based on delivering personalised advertisement on-site (Chaffey and Smith 2013). By using their service, a consumer agrees to be served advertisement as part of the service experience. Lately, however, many of the well-established service providers (e.g. Google) have started offering consumers the possibility to opt out of personalised advertisement. This is a development that has arisen from the data subject's right not to be subjected to automated processing that produces legal effects or significantly affects the data subject (EU Data Protection Directive, 95/46/EC, art. 15). The argument against such a development from industry has been that the advertisement value increases with targeted advertisement; these are funds that can be reinvested for creating a better service experience. Hence, a monetary value can be assigned to the collection, storing and processing of user data. Companies therefore have a direct business interest in learning as much as possible about the data subject, which again clashes with the legal intention in the EU General Data Protection Regulation that "*Data processors, as well as producers of IT systems, should design their services in a data-minimising way and with the most data protection-friendly pre-settings*" (Albrecht 2015). Certain online service providers (e.g. Microsoft) have also launched subscription-based services that are advertisement free. These services, although primarily targeted to business users, offer the consumer an alternative to paying in data. However, online businesses are also giving out mixed messages in regard to the data subject's rights. The EU General Data Protection Regulation (GDPR, or Regulation) will repeal the Data Protection Directive (95/46/EC) (also referred henceforth to as Directive) and entered into force on 25 May 2016. It will apply from

25 May 2018. In a prioritised effort, EU officials are working on creating conditions for a digital single market that includes all Member States. A unified data protection legislation for Europe is the foundation stone in this, for Europe important, effort. Progress was slow and media reported Google, Facebook, and several other top U.S. technology firms, are using lobbyists "*to relax EU privacy laws to suit Silicon Valley businesses*" (Dembosky and Fontanella-Khan 2013). The case of Google is of particular interest, because few companies have been as beneficial in forming the Internet as we know it today as Google has. Let us consider Google's mobile platform Android, the official App Store "Google Play", and their authorisation/identity service. Researchers have found that 73% of Google Play's most popular apps talked to low-reputation websites (those receiving a Web of Trust rating lower than 60/100) while 74% talked to websites containing material that is not suitable for children (Wei et al. 2015). The development of smartphone ecosystems with an abundance of context-aware apps has led to what can be seen as excessive collection of user data. The argument that most mobile app providers need access to the data subject's personal information (e.g. call logs, contacts, photos, location) in order to use a service is in many cases too excessive and uncontrolled. However, all excessive access to user data does not necessarily start with malignant intent, but can be a result of poor planning. The most popular Apple IOS game (according to weekly statistics from the iTunes charts 14.7.2016) Pokémon GO offered two options for users when signing in to play the game. The player could choose between using either Google's authentication service or by registering on the Pokémon website, which was unavailable due to an overwhelming demand. In consequence, players were forced to login using their Google credentials. Using Google credentials required granting the developer of Pokémon Go, Niantic, full access to the player's account. According to a security report on the subject, this included, inter alia, the ability to send and read any emails, images, files, search history, or any previous location data the player has stored on Google's cloud service. Perhaps the most negative aspect from a data protection legislation perspective is that the player was never informed what account rights had been granted to Niantic when logging in to the service in the first place[1]. Studies have shown that users of mobile devices are often unaware of how much data the apps gather, but also dislike the fact when told (Shklovski et al. 2014). A survey by Pew Research Center showed that 81 % of parents "*are concerned about how much information advertisers can learn about their child's online behavior, with some 46% being "very" concerned*" (Madden et al. 2013, p. 61). In an examination of the apps in the Android App store, Google Play, it was found that many apps showed the behaviour of "*overly aggressive communication with tracking websites, of excessive communication with ad related sites, and of*

[1] See security analyst Reeve's documentation for further details, http://adamreeve.tumblr.com/ post/147120922009/pokemon-go-is-a-huge-security-risk, Accessed 14.7.2016.

communication with sites previously associated with malware activity" (Vigneri et al. 2015, p. ii). In their experiment, the researchers installed 2146 popular apps directly from Google Play on a standard Android smartphone and consequently observed their traffic activity behaviour. After executing and interacting with each app that they had installed, they had recorded connections to almost 250000 unique URLs across 1985 top level domains. Official App Store providers (not only Google or smartphone ecosystems) may maintain a position that they give no assurances to consumers in regards to third-party apps. Although they all have a control mechanism in place for accepting apps and are often vigilant when it comes to certain types of content. Still, they seem close to ignorant of the privacy issue experienced by users of their platform. The issue of mass data collection has become a part of life for most smartphone and web users (Vigneri et al. 2015). Grace et al. (2012) categorised three problematic behaviours from analysing mobile in-app advertisements. 1) "*Invasively Collecting Personal Information*", by requesting information not directly useful in fulfilling their purpose. 2) "*Permissively Disclosing Data to Running Ads*", offering direct exposure of personal information to running ads, e.g. for the purpose of circumventing platform permissions. 3) "*Unsafely Fetching and Loading Dynamic Code*", for bypassing existing static analysis efforts by undermining the capability of predicting or confining any code behaviour. Although apps and games are distributed through official App Stores, research still shows us that self-regulation is perhaps not enough in an environment without any de-facto overview (McKinnon 2014). However, it is evident that people continue to use the technologies and applications implicated; otherwise, the said smartphone ecosystems would not continue to flourish. This behaviour is referred to as the "*"privacy paradox" where intentions and behaviours around information disclosure often radically differ*" (Shklovski et al. 2014).

The interesting question from a technical or legal point of view is perhaps not to ask why people continue using these services, although they dislike the privacy violations, but rather how they can be given an option of determining what is processed and communicated about them, while still maintaining their access to current virtual networks and the digital presence in general. For the purpose of technological and social inclusion, teaching children that if the one care about one's own privacy, the child cannot play many popular games or use apps should be considered a discriminatory message that we strongly ought to avoid. Advertisement driven business models are not the issue here, however; the excessive collection of personal information for the single purpose of exploiting the data subject is seen as being in conflict with both current Directive and coming Regulation governing the data protection of data subjects.

1.1. Historical Example of Digitalisation and Regulatory Shaped Development, Creating a Competitive Consumer-First Telecom Market

In the late 1970's, the world started its digital journey, which would change the way we look at privacy forever. One, and arguably the first, example of digitalisation was the digital telecommunication switches (exchanges). Two of the more prominent companies in this development were Ericsson with its AXE switch and Nokia with its DX200 counterpart. In addition to service scaling for operators and improved consumer experiences, the digital telecommunication switch can be analysed through a privacy perspective. The digital telecommunication switch enabled authorised eavesdropping, through telephone tapping, on a massive scale for the first time in history. Although telephone tapping had been possible also earlier in the analogue (circuitry switched) exchange, the digital switch enabled authorities to perform telephone tapping through the telecom operator by automatically recording any calls to and from a certain telephone subscription. There was also an economical enabler involved. Due to the new digital telecom switch, cost efficiency of large-scale telephone tapping was markedly improved. The digital switch removed much of the manual labour in the recording process. The third enabler was an improved quality of service. The analogue system was often more sensitive to noise and as it included more manual labour it was arguably also more error prone.

These three scaling enablers today often define digitalisation: innovative digital services, economics of scale and service quality. These enablers are often the answer to the question how digitalisation is achieved, regardless of domain. The answer to the question what we need digitalisation for, is data, in its various forms. However, the more important question why we need data recorded on everything in life, has a more multifaceted answer that shall be addressed in later sections.

The introduction of GSM wireless network (2nd generation, 2G) technology introduced both new technology and a marked change to the ecosystem of the communication sector. The earlier fixed network (PSTN) ecosystem consisted of three main parties, manufacturers of network infrastructure, operators, and end-users (customers). The operator often had a regional monopoly, the manufacturer had many customers per country, and the consumer had a limited option regarding provider. The GSM wireless network allotted two or more operators to make use of the available frequency bands that were divided by country and not region. The change introduced the consumer to a choice of network operator, which for the first time could be based on personal preferences. Eventually, in many countries, even allowing the consumer the option of phone number portability between operators (e-Privacy Directive 2009/136/EC, recital 47). This option was important, because it removed the last lock-in mechanism available to operators, to "force" consumers to

stay with them. This also indicated the regulator's power to change market dynamics on its own accord. The following years were turbulent for the operators, who experienced a sharp increase in customer churn rates, sometimes resulting in eroding market share and/or revenues. For manufacturers of network infrastructure, the situation changed in the sense that they had fewer customers per country. The technical complexity of the network grew significantly as interoperability and co-existence between the different manufacturers of operator networks had to be guaranteed. This required the introduction of worldwide standards organisations that coordinated the work of defining common design requirements. The technical standards were initially developed and adopted on a continent basis; Europe had the GSM, and North America CDMA. Ultimately, the standards have converged into a global standard referred to as 4G LTE. The reason for GSM's success was, in addition to the industry led standards consortium, a firm understanding and legislation that 17 EC Member States would adopt the common European technical standard in 1987. The Member States then bound their telecommunication operators to adopt the 2nd Generation GSM standard through a competitive tender.[2]

This regulatory environment improved conditions for European manufacturers by increasing the market size, but also created an enriched roaming experience for European citizens. Comparing to social networks of today, the alternative for a non-regulated wireless telecommunication infrastructure would have been that each operator developed their own technology that would be incompatible with all other operators'. This include communicating from one telecommunications network to the other. Such a scenario would potentially have created an ecosystem with a few pan-European or worldwide operators that most likely would have manufactured their own equipment. Such a scenario seen from a business point of view is not perhaps a failure of markets, but from a consumer point of view a drastically inferior experience.

During the past four decades, the world has gone through a technological era sometimes referred to as the digital age. This era has led to a tremendous change in how individuals and businesses manoeuvre in daily life. Yet, across the world, privacy laws, which govern the operational modus for companies providing services to consumers, can originate from a time when the Internet was predominantly used in research labs and academia, if they exist at all. At the time of writing, EU Member State law is regulated through the Data Protection Directive (95/46/EC). The Directive was conceived at a time when commercial activities on the Internet were almost non-existent and the United States have yet to adopt a general data protection legislation. The United States currently rely on sectorial legislation.

[2] See Eliassen et al. (2013) for an extended history of telecommunications sector.

Examining the original underlying network communication Internet Protocol (IP-layer) suggests that the Internet was originally never designed with security or privacy in mind. Rather the technology we now consider the Internet, was designed as a method for allowing as many data packets as possible, from as many nodes as possible, to pass through the network unhindered. Based on these technical design goals we can consider the Internet a complete success. For example, today the data packet delivery time over large distances is limited to a large extent by physical laws and not by technological constraints. However, the impossible task of foreseeing the impact of Internet on our social constructs has to a large extent directed continued academic research in the area, towards trying to solve the issues of security and privacy that the initial communication protocol stack did not consider. Arguably, much of this research is based on the assumption that anonymity, in its various forms, is achievable and desired.

1.2. Introducing Intelligent Offerings in a World of the Internet of Things

Today the Internet has become a global platform for commerce and communication. At the same time, the regulator has lately not been absent, but clearly more careful of business interests than consumer choice, compared to the onset of the digitalisation process. Looking forward, we can anticipate that intense technological progress will continue to shape new domains in our lives. It is predictable that, within the coming decades, this will extend to include many other areas, e.g. personal healthcare and home automation. These new domains will introduce a myriad of highly sensitive information sources, information that must be processed, and often stored for an indefinite and sometimes an infinite period in order for these areas to be digitalised. By embedding information-sharing electronics into everyday physical objects, we will create a "*global cyberphysical infrastructure*" (Miorandi et al. 2012). The term often used for describing this future Internet vision is the Internet of Things (IoT). Internet of Things is based on standardised communication protocols and merging computer networks into a "*common global IT platform of seamless networks and networked "Smart things/objects""* (Vermesan and Friess 2011 , p. 10). From the perspective of platform and service innovation, by utilising Internet of Things technology, the focus will be on creating intelligent services that are able to draw inferences from our own and other's data. This will offer users descriptive answers, predict future behaviour and needs, and eventually provide prescriptive suggestions for improving daily life. Intelligent platforms and services are thus defined as analytics enabled platforms and services.

As the development of the underlying Internet technology showed, introducing security and privacy measures later on is very difficult in a distributed environment.

Changing the IP-layer, which would potentially introduce more built-in security into the protocol, has been an ongoing endeavour for the past decades[3]. Without incentives to implement privacy friendly solutions, the change may not come. Particularly, when the companies that are the leaders of digital platforms and services are not of European origin, they might not share the values and ideals of the European society. For this reason alone, if the EU citizens and voters share the values of strong digital privacy rights, then enforcing them through legislation benefits society at large.

As later discussed, data protection as a legal term in EU legislation considers personal data that is linked to a natural person. Data protection legislation has a foundation in the European Convention on Human Rights, Article 8, the Right to respect for private and family life.[4] The article is often referred to as establishing a 'right to privacy'. Privacy as a philosophical term has long roots and many diverse definitions. Parent (1983) defines privacy as "*the condition of not having undocumented personal knowledge about one possessed by others. A person's privacy is diminished exactly to the degree that others possess this kind of knowledge about him.*" He highlights that the condition of privacy should be detached from the right to privacy. Schoeman (1984) divided earlier philosophical research definitions into three main branches. 1) Claim, entitlement or right to privacy. 2) A measure of control an individual has over data connected to himself, the level of intimacy (sensitivity) of such data, and who has access to such data. 3) A state or condition of limited access to the individual.

The European Convention on Human Rights may grant the right for privacy, but understanding what this means in a digital environment, where data are collected in an ever increasing manner and this data are then processed tirelessly by smart algorithms, is important. The European Data Protection Supervisor (EDPS) considers that achieving better respect for and safeguarding of human dignity could be the counterweight to the pervasive surveillance and asymmetry of power that now confronts the individual (Buttarelli 2015). An ethical framework needs to underpin the building blocks of this digital ecosystem. The EDPS opinion sets out to open up the discussion of what should be at the heart of a new digital ethics framework dealing with intelligent offerings. The thesis aims at continuing this discussion by elaborating selected areas important for empowering the individual and improving conditions for launching competitive services. As later discussed, the current proliferation of cloud-based 'X-as-a-Service' is here considered to pave the path towards a digital environment that enables digital personal assistants as

[3] An early draft version of the IPv6 specification was given by Hinden in October, 1994. For further details, see, https://tools.ietf.org/html/draft-hinden-ipng-overview-00, accessed 14.7.2016.

[4] See the European Convention on Human Rights, accessed 3.11.2017 http://www.echr.coe.int/ pages/home.aspx?p=basictexts/convention

recommenders offering decision support and eventually as expert actors on the behalf of an individual.

1.3. Research Agenda

Brynjolfsson and McAfee (2014, pp. 123-124) make the argument that we as a society need to define "*what we really value, what we want more of, and what we want less of*". In their world, technological progress cannot and should not be hindered. At its inception, the Internet and its related activities were considered to be of a free nature. Trust and practicality issues with payments contributed to an environment where only meagre revenues were created. Over the last decade, we have been able to witness a change in the generation of revenues; companies such as Google and Facebook are generating persistent and large positive cash flow from predominantly free digital services. At the core of these so-called free business models is that, while users are not charged money for using the service, they allow the service providers to process and sell information about them (McGrath 2010). Companies with an online advertisement based business model, like Facebook and Google, share their insight from collected customer data with a multitude of affiliated companies (Gomez et al. 2009). A monetary value can thus be assigned to the collection, storing and processing of user data (Smith et al. 2011). Ausloos (2012) argued that personal data has now become the new currency on the Internet. The opposing argument presented by incumbents, is that by using digital platforms the data subject gives permission to the controller of these platforms to use the personal data in order to be able to provide tailored services. Provided the service is of value to the data subject, the service provider owns the data (information, knowledge) they have synthesised by working on the personal data with their algorithms.

At the same time, security for everyone involved is becoming ever more important as we over the coming decades move towards becoming a near fully digitised society. Security, defined here in broad terms as comprising the security of digital life in general, has also been afforded attention by EU lawmakers as it launched a Directive on Network and Information Security (NIS) (EU 2016/1148) [5]. The regulator considers undesirable occurrences to information systems caused by human mistakes, natural events, technical failures, or malicious attacks, as security incidents. The handling and mitigation of negative effects in the case of a security incident are hence outlined by the Directive on Network and Information Security. NIS provides legal measures to improve the overall level of cybersecurity by enhancing cooperation, ensuring risk management practices in key sectors, and by increasing the cybersecurity capabilities in the Member States (European

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Commission 2015). In 2016, Internet users were made aware of several large breaches that had occurred years earlier. Companies such as Yahoo and LinkedIn revealed that data concerning more than 1 billion accounts (Thielman 2016) and 167 Million accounts (Hackett 2016) respectively had leaked from their systems. Together the NIS and the GDPR should compel companies to come forward earlier with data breaches. However, as the examples above indicate, once a network breach happens it may be detected too late with conventional passive network security methods. In chapter 5 we describe methods for going beyond conventional methods and introduce the term active network security, as to identify the paradigm shift in the view of network security. Section 7.2 summarise, in the form of a taxonomy, active network security developed on the basis of the explorative case studies in chapter 5.

The primary focus of the thesis is to improve the understanding of the role that privacy legislation [6] plays in discovering an equilibrium for the rights of different stakeholders, without limiting future opportunities for developing desired intelligent services. Driving the regulatory development of data protection connected to intelligent service development, we find profiling and automated processing, and closely related fields such as tracking and giving consent. By investigating current information system literature, we determine what is meant by intelligent services and intelligent systems; hence, we gain a grounding in the area of analytics that guides the development of intelligent systems. Considering the broader perspective of privacy, the thesis aims to also make a contribution in what type of security measures should be considered adequate.

International e-commerce implies cross-border data flows and the privacy challenge will therefore be to construct a global legal regime that would provide data subjects control over their personal data, and at the same time allow companies the ability to engage in trans-border data flows (Birnhack 2008; Regan 2003). Determining a stable globally viable state requires a broad understanding of issues such as IT-security, intelligent services, and scalable systems. The technical aspects ought to be treated as being intertwined with the legal texts and regulatory intentions. To understand and determine the technical challenges facing organisations building intelligent services and platforms in general, certain technical areas are examined. The selected areas are scalable system architectures, network intrusion detection using big data tools, and the creation of active intrusion defence methods. These areas provide industry with advances in securing user data, and thereby improving user confidence over time. However, these methods should not be considered as the only means of improving security, but rather provide industry and academia with new avenues in improving security. The GDPR (art.

[6] The term 'privacy legislation' is used to indicate that there are other considerations to be made, than those included in the general data protection regulation, e.g. NIS Directive and Directive on Privacy and Electronic Communications (2002/58/EC).

5(1)f) does not define the level or type of security, but states that data shall be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing.*" We can assume that what is appropriate will evolve over time; therefore documenting current state-of-the-art security methods also serves a historical purpose.

The current EU Data Protection Directive (95/46/EC) that forms the basis for today's legislation in the separate EU Member States is considered problematic primarily due to the fragmented adoption in national laws. A directive does not supersede national law, but rather sets a general rule and goals to be transferred into national law at the national legislator's discretion. This may lead to a difference in interpretation and/or implementation between the Member States. Hence, contributing to the fragmentation. Therefore, to solve this problem an EU-wide General Data Protection Regulation has been adopted to replace the Directive.

The reform of the data protection legal framework has been met with considerable discussion regarding its objective. The Regulation supersedes incompatible Member State law and will also influence companies established outside the EU if they handle personal data regarding individuals residing in one of the EU Member States. A regulation can be compared to a national law, but the regulation also binds all Member States to adhere to the same law text. Wagner and Benecke (2016) argue though that the GDPR will give Member States some latitude to enact further legislation; one such area is processing and freedom of expression and information (GDPR art. 85). Still, the purpose of the reform has been to improve the clarity and coherence of personal data protection by strengthening individual rights and reducing administrative formalities for companies. Writing legislation for an area under intense development has been challenging; although most parties agree that the current Directive is cumbersome to administer, it is not clear whether the Regulation will improve the situation. The EU Commission sped up the reform process considerably in 2015 by launching the EU digital single market strategy. From the perspective of a digital single market, the new Data Protection Regulation is essential when compared to the current EU Data Protection Directive. Nevertheless, the Regulation still lacks clarity and protection in some cases, but perhaps also includes a faltering rationale (Enkvist and Westerlund 2013; Westerlund and Enkvist 2013; Westerlund and Enkvist 2016).

Wallgren (2004, p. 602) considered that legislation is under strain due to how digitalisation changes the underlying foundations of society and its interfaces to the digital world. He states that from a legislation point of view, the ever-accelerating pace of a complicated technical environment leads to "*that traditional means of solving legal problems are becoming less efficient*". Sandgren (2000) urges the research community to search for new tools through an empirical legal science method. He finds that jurisprudence is at risk for marginalisation unless it takes on the development in other fields. Wallgren (2004, p. 603) considers that the

traditional approach to legislative development in the case of information and communication technology is already limited. The reason for these shortcomings of the traditional approach he defines to that "*the IT sector tends to offer solutions of a complex nature and the lawmaker often encounters problems in trying to satisfy the prevailing demands*".

The historical relation between the fields of Information Systems and Legal Science are readily observable in the digital world. Information systems theories in generative digital infrastructures have its origin in the field of Law (Lessig 1995, 1999, 2006; Zittrain 2006). Henfridsson and Bygstad (2013) identified three generative mechanisms at the core of creating successful digital infrastructures: innovation, adoption, and scaling. These mechanisms were considered self-reinforcing processes that create new recombinations of resources. As user adoption increases, more resources are invested into developing the service and therefore the usefulness of the infrastructure increases. True service scaling attracts new partners by offering incentives for collaboration and increasing collective rewards. Considering that the assumption made is correct, then the theory of the generative mechanisms for digital infrastructure is a representation of how successful digital platforms are flourishing. Hence, the inferences to be made are not only technological but also socio-economical.

The primary object of study is the European Union regulation for data protection. The legislation affecting the digital world is however based on a number of laws and therefore this study will consider other laws when relevant. At the core of current and future digital platforms and services are the privacy rights of the individual stipulated by privacy legislation. Therefore, the focus will be on resolutions for a focused view of how data subjects can be given the control of their digital presence. All data subjects in the EU should receive the same level of protection, but companies should also be able to compete on equal terms. Currently, incumbents can protect their business models by not allowing competitors access to their platform. Once a platform reaches a critical mass of users, the immobility of data outside the platform becomes what can be seen as a lock-in mechanism. This lock-in mechanism should be studied further to understand why it contributes to a problematic situation for the future adoption of intelligent services.

1.4. Research Questions

The field of study directs the research questions towards an understanding and improvement of legal and socio-economic arrangements, supported by technical augmentation. By exploring ways of interpreting the data protection legislation in relation to intelligent systems, I expect to achieve a deeper and more meaningful understanding of the complex interdisciplinary phenomena of trust for digital platforms and services. Trust in a social context often carries a moral value and is

frequently seen as a continuous function (i.e. in various levels of trust adjusted over time). Trust arises from the risk of being let down and without this risk, trust would serve little purpose. For humans and animals alike, trust enhances relationships. Certain activities have naturally, over the millennia's, evolved as being most efficiently handled within a cohesive social group (Marsh 1994). Trust originates from the concept of family, both as a way to ensure that offspring survives but also because of self-preservation through the sharing of food. Through experience, we learn to apply trust of various degrees in our relations.

In a technical context, on the other hand, trust is often defined as a binary representation. In network security research, we often try to classify a user either as malicious or good (normal). A platform or service is likewise also often considered either trusted or not. Examples of this thinking are, for example, ranking sites such as TRUSTe[7] and Web Of Trust[8], but also issuers of security certificates (certificate authority). However, this binary thinking is likely to contribute to the privacy paradox. One may consider a social network platform trusted when it comes to handling network connections and simple messages within the network. When the platform extends its service beyond messaging into, inter alia, news delivery, image sharing, payments, direct marketing, and delivery mechanisms for virtual reality, then it becomes difficult to discern between the initial trusted platform and a myriad of potentially untrusted practices. Because of the non-transparent activities taking place, the question of how personal data are shared and processed, and for what purpose becomes an issue. Ranking sites may give the platform the highest score and the platform may be a root certificate authority (Leyden 2017), but this offers little improvement to platform transparency and trust. The more artificial intelligence that is built into the platform and the more data sharing activities between the services on the platform, the more it is likely to undermine trust for the digital platform further. Recent research into the accountability of algorithms, although outside the scope of this thesis, may provide a new dimension for understanding the issue of trust for intelligent services (Diakopoulos and Friedler 2016).

The introduction of cryptocurrencies (such as Bitcoin) are based on the premise that trust can be achieved through consensus, also referred to as trustless consensus (Nakamoto 2008). Through the use of smart contracts (a contract written in a programming language and executed on a virtual machine connected to a blockchain) that are enforced through a consensus mechanism, it was hoped that the risk of performing transactions would be nullified. As most interactions with an information system is of a transactional nature, trust would be built into any system utilising blockchain technology. However, blockchain technologies that implement the consensus mechanism are not infallible either. Experience from the Ethereum blockchain shows that trust is still needed both towards those that support the

[7] See https://www.trustarc.com/

[8] See https://www.mywot.com/

technology through processing transactions and those that craft the contracts (Spode 2017). In addition, any boundary service interacting with the blockchain would potentially disrupt the trust mechanism if the boundary service output cannot be verified by the blockchain. Elimination of the transactional risk may one day be achieved, but for the foreseeable future, trust remains an important topic in the understanding of platforms and services.

Merging the social and technological views on trust is perhaps not possible, but a better understanding of how to achieve an improved level of trust in the interaction between technology and people should prove valuable to both the legal and the information systems research communities. At the core of this study is the role a digital platform plays in facilitating said interaction in relation to the Data Protection Regulation. Four research questions that are intended to probe the ability to construct trusted digital platforms and services are put forth.

RQ 1. What are relevant interpretations and ambiguities for information systems that can be derived from the GDPR, particularly in regards to such processing of personal data that leads to profiling and automated processing?

RQ 2. What future technical implications can "appropriate security", defined as a legal requirement for lawful processing under GDPR, entail for scalable information system architectures?

RQ 2.1. With focus on security in publicly accessible software, what is a viable technology basis for a scalable processing architecture?

RQ 3. What is a potential future direction for EU privacy regulation in guiding the continued development of digital platforms?

1.5. Research Theory and Methodology

Studies in information systems are often of an interdisciplinary nature and this dissertation is not an exception. The research field of information systems is often defined as an intersection of information technology, business, and data processing (Thomas 2005). In this study, the business dimension is defined more broadly to also encompass the social environment. Governed by legislation, this is the environment where humans, technology, and algorithms interact in and that companies profit from. Digitalisation causes a considerable amount of stress on this environment, stress that takes different forms depending on the field of view, but nevertheless constantly works to reshape the environment. Sandgren (2000) considered studies in a closed specific field to often have a tendency to try to define the problem so that it conforms to existing tools. For example, jurists tend to fit the

problem to the legal method or engineers to a solvable technical problem. He defined this in terms of the legal method that has its limitations in that it cannot deliver results for a problem, which is not taken up by positive law. To achieve interdisciplinary research in information systems, we should try not to limit the research by applying any of the individual tools provided either by other fields or by our own. Rather, we should critically examine our tools in order to find new ones that more fluidly accommodates alternative forms of knowledge production (Grover and Lyytinen 2015). Grounded research methods in information systems are well established. Descriptive or normative methods have perhaps still not established themselves at the same level when it comes to traditional information systems research.

However, not only information systems face the challenges of methods/tools that do not always fit the underlying problem. The legal sciences have long struggled with incorporating the mitigating effects of digitalisation into law texts. An example that Seipel (2004, p. 31) provides is the difficulty of classifying the new information society related texts. He states that some traditionalists argue that IT law should be fragmented and only deal with specific issues involving computers. He refers to legal informatics as an encompassing field of view of "*how rules interact with tools*", where IT Law is a part. This later view is also the approach followed throughout this work.

The thesis is based on a combination of research methods from the investigated fields. The discourse of the thesis is largely based on methodology used in the legal informatics field. The reasoning behind this choice is that the study (lex lata) and resolution (lex ferenda) is primarily defined through argumentativist legal dogmatics and de lege ferenda, how the legal framework ought to be adapted to fit the described environment. As shown in section 1.5.1, the legal methodology is then extended by empirical technical case studies, as a supportive argument that was suggested by Sandgren (2000). For the purpose of this thesis, these empirical studies can be defined as exploratory case studies into various areas relevant for delivering a normative discourse in regards to future regulation. It is acknowledged that the approach is exceptional in the field of information systems. However, Wieringa (2014, p.35) highlights that traditionally, design science research projects have always taken place in a normative context of laws. The connection to design science is elaborated further in section 1.5.1. Also to its support, Sørensen and Landau (2015) sought to develop the information systems understanding of possible relationships between a field and its practice context. Yoo (2013) has added to the debate by seeking current technological developments that stretch the boundaries of the information systems field. In order to determine the regulatory objective and technological implication, the field considered as an object of study is the legal sources surrounding data protection.

To regulate implies that a method is defined, and in this thesis, the regulatory method primarily considered is the GDPR. Råman (2006, p.30) considers that

regulating software and in particular secure software, require a definition of regulation that:

> "is 'decentred', i.e., diffused throughout society. A wider perspective, which deviates from the pure state-centred regulation, is necessary in order to understand the wide area of information security and especially the regulation of secure software development. This regulation is essentially dispersed in different types of self- and governmental regulation, and social norms which have similar and even forceful effects to secure software development. Technologies and methods for their development also play an important role."

A decentred definition adds additional ambiguity by stating that the method provided in the form of a law cannot be considered complete. This seems to have been the legislators' intention regarding the GDPR as well, as the EU Commission should for example continuously monitor whether the digital landscape in third countries offers an adequate level of data protection, and may later introduce additional limitations, obligations, or opening up access to a third country. In concert with external stakeholders, the Commission also seeks to define standards for certification mechanisms and portability guidelines.

The sought solution in the thesis is a technorealist view that elaborates the role digitalisation plays in human evolution and everyday life. "*Integral to this perspective is our understanding that the current tide of technological transformation, while important and powerful, is actually a continuation of waves of change that have taken place throughout history*".[9] The technorealism principles have received criticism from an engineering perspective by Holmes (2003). However, what it can offer in jurisprudence analysis, is a middle ground between the views of techno-utopianism, "*the belief that advancing technology will automatically bring global prosperity*", and neo-Luddism, "*the belief that global prosperity can be achieved only by rejecting technology*" (Holmes 2003). Holmes redefinition of the principles serves to elaborate the role of humanity in the design process, whereas the original work sought to highlight the increasing importance of daily life being determined by information flows and consequent algorithmic decisions. The aim of technorealism is to understand technology and apply technology in a manner more consistent with basic human values. Holmes may be correct in the sense that humans create the technology used today; however, the original technorealist movement identified the information flow as a driving force for change in our social environment. A more modern terminology than information flow could today be defined as big data and big data analytics. Depending on the view, these automatic decision-making algorithms today help or control the individual with anything from driving to shopping, and thereby affecting a change on every single individual that participates in using this technology. The thesis does not take a position on the moral implications or completeness of the technorealism principles. Rather, the principles

[9] See Technorealism. (1998). Accessed 22.09.2017, www.technorealism.org

are seen as a sober view of reality and going forward they offer a view of digital social inclusion contra rejection of coercive persuasion.

The population primarily considered is the European Union Member State residents. Their privacy ethos spans the wide range from completely transparent to non-users of digital provisions. The population distribution is unknown; however, the normative discourse must work to embrace all. Other stakeholders are also considered when relevant. There is no distinction made between regulator and other legal sub-stakeholders. However, it is worth noting that laws are passed by politicians and not legal scholars. Therefore, a law when passed might be formed with an agenda that is not evident to those writing and upholding the same law. The difficulty of distinguishing the role different parties play in the law making process, makes it necessary to treat them as one and this is also reflected in the legal policy discourse.

1.5.1. Towards an Interdisciplinary Research Theory for Information Systems and Legal Research

Wieringa (2014) defines design research as the design and investigation of artefacts in a context. He draws two separate avenues for the design research process, the first starting with a design problem and the second with a knowledge question. The former is addressed through a design cycle that focuses on problem investigation, treatment design, and treatment validation. In software engineering the treatment term is often referred to as the implementation. The other avenue, to answer a knowledge question requires problem analysis, research setup design, validation, research execution, and data analysis. Both avenues also include application of theory.

Design science offers information systems research a methodology to investigate observed problems when developing a better understanding of mechanisms that exist in the interaction between the artefact and its contextual environment. The identification of stakeholders is important, as they often define the requirements that should be addressed. The requirements are also important in the validation process. The research methods for the individual papers are further described below, but the thesis as a whole takes place in the normative context of legal acts that govern the digital landscape, but naturally also in the context of ethics, human values, desires, and goals that constantly evolve with the individual and cultural groupings. As such, a common natural stakeholder may be difficult to define. However, I assume that the primary stakeholder is the lawmaker and the requirements presented are the legal acts and other legal tools such as norms, opinions, and court resolutions. Another stakeholder may be a company or individual affected by the legal acts. However, defining their view may be difficult to generalise. These actors

can be used when reflecting upon the societal effects of a particular issue or question and then analysed in that specific context.

The positivistic approach would be to accept the legal acts as infallible fact, and an external viewpoint analysis may offer some information systems design insights, but minor scientific output. The external point of view here refers to the legal term for outside examination into a specific set of laws. Hart's (1961, 1994) positivistic approach assumed instead a combination with an internal viewpoint (Holton 1998). As the chosen point of study is primarily external (the mechanisms of information systems in combination with the GDPR), a normative theory based on examining the problem through what can be considered a holistic approach is chosen. This includes the law text, other legal tools, technology, and an economical aspect through theories regarding platform economy.

Mäntysaari (2017, p. 145) defines a User-friendly Legal Science theory that realises the qualitative approach of design science. He considers a positivistic approach in for example economy or analytics to be based on methodological individualism and a narrow view on societal reality, whereas, "*User-friendly Legal Science has as its goal interpretive understanding, takes a holistic approach, and tries to describe societal reality from different perspectives.*"
Mäntysaari (2017) reflects on the difference between User-friendly Legal Science and traditional "*law and something*" legal theories[10] in regards to what can be used as primary sources. Whereas the later often connects an external view with a specific primary source, the former opens up for a wide variety of sources relevant to a holistic description and understanding of the problem at hand. User-friendly Legal Science also considers the role of legal dogmatics important as it offers a middle ground (debate topic) between law and practice.

In User-friendly Legal Science Mäntysaari draws parallels to the legal history discipline, where questions concerning how law has evolved and why they changed are asked. The questions are then answered through the hermeneutical circle, by legal historians trying to understand and describe how earlier legal systems work. The method theories of legal history are diverse, e.g. doctrinal study, connectivity to current law, societal impact, as well as statistical and economical approaches. The ability to choose between multiple perspectives and diverse sources are well suited for creating a balanced narrative, thus also rejecting legal positivism, as choices preceding the research reflect the researcher's subjective values. User-friendly Legal Science approaches the problem similarly, by determining a holistic perspective it sets the goal as interpretive understanding by describing social reality from different perspectives. (Mäntysaari 2017, pp 137-147)

[10] "Law and something" legal research are often based on a generic theory referred to as the legal method or legal science. Legal informatics can be considered such a field that Mäntysaari refer to as "law and something", i.e. law and information technology.

Research questions in User-friendly Legal Science are still recommended to be sufficiently narrow, regardless of the holistic approach to answering them. For the purpose of an interdisciplinary thesis, User-friendly Legal Science offers a bridge between a fervently theory driven field such as information systems and a more practice and policy driven field such as legal science. An adapted User-friendly Legal Science theory thus offers the thesis a theory connected to information systems, through design science, by including relevant technical single-case studies. The case studies are of an exploratory nature, intended to identify single case mechanisms (Wieringa 2014). The thesis as a whole is therefore based on a descriptive part and combined with an interpretivist part that includes problem solving as suggested by Mäntysaari (2017, p.145).

The evaluation for descriptive design science was characterised by Verdonck et al. (2015, p. 12) as

> can be done through scenarios, where the utility of the artifact is demonstrated through detailed scenarios, or through informed arguments, where information is used from the knowledge base (e.g. relevant research) to build a convincing argument for the artifact's utility.

There are different legal dogmatics methods, some of which have been defined as argumentativist, realistic-technological, and critical legal dogmatics (Vaquero 2013). In this thesis, these methods are mostly considered normative and descriptive, and are referred to in a general sense as legal dogmatics. This is in accordance with Peczenik's (2005) view that legal doctrine can be descriptive and normative at the same time.

To achieve a deeper understanding from an external point of view, formulated problems can also be studied through technical case studies. New open problems can be identified in this process through an iterative approach. To achieve the interpretive understanding in User-friendly Legal Science theory, one can make use of a constructivism based method theory. From the legal perspective of the whole thesis, using an observational method in order to explore an artefact in its environment offers a way to evaluate technical case studies. It should be noted that the information system approach to observational case studies tend to often be action research based. Although the User-friendly Legal Science theory is defined through the pragmatical school of thought, the quantitative perspective is suggested to be examined in individual studies, whereas the thesis as a whole uses a qualitative perspective. This is argued to be based on the premise that complex societal phenomena would otherwise be lost. The constructivist method of answering questions through a holistic approach and repeating the hermeneutical circle until sufficient knowledge is gathered to present an answer is considered the basis for User-friendly Legal Science theory building. Although going beyond the traditional scope (Law and IT) this theoretical approach can be considered well suited for legal informatics. Integrating the social and economic dimensions may in general

improve the basis for reasoning about complex concepts related to digital platforms. In reference to the conformity limitation identified by Sandgren (2000), User-friendly Legal Science may offer the ability to study a phenomenon more broadly and thereby avoid the tendency to try to define the problem so that it conforms to the existing tools.

1.6. Overview and Contribution of Papers

The thesis includes six original research publications, published in peer reviewed scientific journals (3/6) and at peer reviewed conferences (3/6). The journal articles are from the field of law and focus on the EU General Data Protection Regulation. I have presented the three conference publications at international conferences. The topics for the conference publications have been chosen to elaborate new technical innovations that at the time of publication lacked academic contributions and understanding. The papers are presented thematically, first the law related papers and then the technical explorations. Table 1 shows the link between original publications and research questions posed.

Table 1 - Original publications and the research questions they address

Publication	Research Question
Paper I: Enkvist, J. and Westerlund, M. (2013). Personuppgiftsskydd – med särskild betoning på profilering, *JFT – Journal of the Law Society of Finland* (2)2013, pp. 85-113.	RQ1
Paper II: Westerlund, M. and Enkvist, J., (2013). Profiling Web Users – In light of the proposed EU Data Protection Regulation, *Retfaerd - Nordic Journal of Law and Justice*, Vol. 36, Nr 4/143, pp. 46-62.	RQ1,RQ3
Paper III: Westerlund, M. and Enkvist, J. (2016). Platform privacy: the missing piece of data protection legislation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7(1)2016, pp. 2-17.	RQ1,RQ3
Paper IV: Westerlund, M. Hedlund, U., Pulkkis, G. & Björk, K-M. (2014). A Generalized Scalable Software Architecture for Analyzing Temporally Structured Big Data in the Cloud. *New Perspectives in Information Systems and Technologies*, Volume, 559, Springer.	RQ2,RQ2.1
Paper V: Xiang, J., Westerlund, M., Sovilj, D., and Pulkkis, G. (2014). Using Extreme Learning Machine for Intrusion Detection in a Big Data Environment, *7th ACM Workshop on Artificial Intelligence and Security (AISec14) collocated with 21st ACM Conference on Computer and Communications (CCS14)*.	RQ2,RQ2.1
Paper VI: Paarnio, P., Stenvall, S., Westerlund, M., and Pulkkis, G. (2015). Active Intrusion Management for Web Server Software: Case WordPress, *Tenth International Multi-Conference on Computing in the Global Information Technology (ICCGI 2015)*.	RQ2

1.6.1. Legal publications

In the first publication (in Swedish), Enkvist and Westerlund (2013) examine the then newly proposed regulation. The work primarily deals with defining the terminology and understanding the scope of the proposal. In the paper, the interpretation primarily focuses on profiling of users. The work and insights are closely connected with the fourth technical paper, as I there gain an understanding of how massively scalable systems are to be built. The paper also connects the 'profiling' term to the field of analytics and motivates the relevance of the new regulation. Towards the end, the paper identifies some limitations, for example in relation to profiling of "virtual identities". The paper is mostly based on descriptive methodology, by analysing positive law.

The second publication (Westerlund and Enkvist 2013) continues with the theme by analysing what profiling of web users means in light of the proposal. The paper uses the hermeneutical circle method to identify ambiguities in the interpretation of

the proposed Regulation. One of the identified issues with the proposal was the vagueness regarding what is meant by profiling that produces legal effects and what is meant by "significantly affects" a natural person. We also motivate further our previous findings from the first paper relating to the lack of protection of virtual identities. We highlight that often the physical identity would not be needed by the controller/processor for user profiling and the consequent customisation of content to users.

The third publication (Westerlund and Enkvist 2016) takes place just before the introduction of the final revision of the proposal to the EU Parliament. As the proposal has matured, we study its impact on the digital platform and find that the legal tools required are still largely unspecified. The paper adopts a critical legal dogmatic methodology and our findings lead us towards asking if the rationale for the regulation is old-fashioned, even before its adoption. When considered through the theories of the platform economy, we reflect on if the regulation should have been formulated differently. The paper provides certain scenarios and propose suggestions as to how digital platforms should be regulated to improve the protection of data subjects. The main critique presented is in relation to the ability of digital platforms to create "data silos" and hence lock-in its user base.

1.6.2. Technical publications

The thesis also includes three technical single-case studies. The choice of topic for these papers has mostly been curiosity or problem driven and can be best defined as single-case mechanism experiments through the design science methodology (Wieringa 2014).

In the fourth paper, Westerlund et al. (2014) propose a reference design for a scalable processing architecture using cloud computing. We develop a prototype to advance the understanding of technical challenges involved in creating a massively parallel processing software. In the paper, we first define a general workflow for temporally organised data and as a solution, a component abstraction for generalising the insights learned from the constructed software. In addition we draw general security conclusions based on our design.

The fifth paper (Xiang et al. 2014) develops a machine learning algorithm for performing analytics on an open-source big data platform (Hadoop). To validate the ability of the algorithm we analyse a common dataset used in network security. We show that our implementation of the extreme learning machine scales with the increasing of processing nodes. An insight with relevance for the GDPR that can be drawn from our paper is that active network security is a viable option for securing company data. Traditionally, using passive network security methods was considered enough, but this is a slow method to detect intrusions with. Thereby, network intrusions often result in massive data loss. Today machine learning

methods can be used to perform big data analytics in near real-time, and should be considered to be included in a company's network security arsenal.

The sixth paper (Paarnio et al. 2015) investigates how to improve security in the world's most popular content management system, WordPress[11]. WordPress is well known for numerous plug-ins of varying quality, and as a result that often opens up vulnerabilities that are used to take over the service or leak data. We developed novel methods for WordPress called booby traps. Booby traps are implemented as an active defence against intrusion attacks using return-oriented programming. The methods may offer improved protection for zero-day attacks and the ability to classify certain connections, e.g. those scanning for specific plug-ins, as suspicious. We estimate that our methods should be generalisable to other web server software. The work shows that largely unexplored avenues in securing web services still exists. So far, the economic incentives to use this type of technology may have been missing, and SME companies using open-source software have often relied, perhaps too much, on the community to provide secure solutions. Redefining what constitutes state-of-the-art security, which companies need to employ in order to comply with the GDPR, can perhaps improve the situation and increase the needed funding for open-source software organisations.

1.6.3. Limitation of Scope and Legal Disclaimer

The research questions are constricted and the scope of the thesis is limited, though the traversed field is more ambiguous and broad than the typical environment construed in a doctoral thesis in information systems. However, I find this warranted in order to be able to extend information systems research toward an unbeaten track. The regulator (EU Commission) has set itself a lofty strategy in creating a digital single market, with the GDPR as what can be considered the fundamental regulation. The GDPR and other legislation interacting with technology, offer the information systems discipline a new domain for investigating wicked problems. This thesis is but an example of what can be researched in this domain. History shows us, as stated in section 1.1, that the presence of an active regulator requires digital innovation research to acknowledge that the environment is broader than only technology and economical quandaries. Definite answers are difficult to achieve in this area and as often is the case in any technology requirements documentation, the law in itself is not always self-explanatory or definite. Therefore, we limit the discussion to some aspects of the law and the defined environment.

The Data Protection Regulation has gone through several iterations during the time of research. Therefore, some of the papers may refer to a situation or topic no

[11] Based on W3 Techs ranking of content management systems, accessed 28.07.2017 https://w3techs.com/technologies/overview/content_management/all.

longer relevant. Still, this should be considered as affirmative progression, as the outcome of research then has had an impact.

A doctoral thesis in legal science that reference legal sources from different judiciaries often derive the philosophical differences of both the judicial systems and the legal scholars. The author acknowledges the judiciary differences between US law, central European law, and Nordic (Scandinavian) law. The heritage of the Nordic judiciary view is self-evident in this work's view of trust in society, individual freedom, and the role of state as an active participant. The inclusion of U.S. law scholars serves as a historical reflection on the regulatory development of cyber law.

The individual papers or the thesis as a whole should not be considered as legal advice in any form.

Facebook is at the forefront. It's the company that can fundamentally change the way information is being exchanged and processed. It can be the basis for artificial intelligence to develop over time.

—Yuri Milner

2. Evolution of Big Data Analytics Enabled Platforms

Information systems may by the layman often be described as something complex, mysterious and to a part elitist in the sense that only a limited group of people tend to comprehend them. When information systems are treated as a whole, this is often an earned reputation. Due to the design principles often used for scalable software, transparency issues in the field are well known and are often reported in media as security incidents or design flaws (Tanenbaum and Van Steen 2007, pp.4-7). To comprehend the problem setting present in the new regulatory environment, this section presents a technological background as to provide the basis for the multi-disciplinary research objectives and research questions. The underlying issue that this thesis considers is that companies are constantly compelled to improve turnover, and becoming increasingly data driven often allows these companies to improve their businesses. However, this should not automatically imply that any type of data processing should be allowed, or that the results produced should be used to the detriment of the individual. Data protection also implies that data are securely stored, something many companies and other institutions today struggle with (Takabi et al. 2010). In addition, as discussed later in chapter 3, 4, and 7, data protection implies that personal data can be transported freely between platforms, without unnecessary obstacles put in place because of business reasons intended to strengthen the platform's control of the user.

This section presents the development of fields highly relevant to the systematic evolution behind the data driven business model. The intention is to present the gradual development occurring in information systems and connecting the development to the GDPR. Although to the untrained eye it may seem that a technological revolution would better describe this change. The sections of this chapter that present the individual techniques and technologies show that they either have a history, sometimes spanning several decades, or represent a logical next step. The evolution observed is arguably mostly taking place in the combination of these technological resources. The focus is on topics considered relevant for the development of intelligent platforms and services. In addition, the network security aspect of the thesis and a link to platform economy theories are introduced. The chapter reviews the evolution of intelligent systems through the perspective of information systems and the consequent development of the analytics field as a driver for future development.

2.1. The History of Analytics

Analytics as a field has a history in operations research (also referred to as management science). Operations research in turn has long traditions going back to first improving military operations (Morse and Kimball 1946) and later on as a science for taking business decisions (Ackoff 1956), such as improving manufacturing performance. We often see operations research and decision theory defined in two main branches; descriptive or prescriptive/normative. The core difference between these is in the definition of the data subject; prescriptive assumes that the subject acts rationally and that analysis of the group gives insight into the individual, while the descriptive assumes that the subject is irrational and requires analysis of the individual subject in order to gain insights into its behaviour. Descriptive questions in an Internet setting usually relate to earlier behaviour of the subject, e.g. how to cluster the individual based on products earlier viewed or on entered search terms. Prescriptive modelling on the other hand is often concerned with improving or changing a process. A typical use of prescriptive methods in this context relates to using optimisation techniques for improving the customer experience. (Delen & Demirkan 2013)

A third type of decision model has been proposed to deal with probabilities of future events, namely predictive modelling. Predictive modelling being the least explored field of the three, has had some difficulty in finding an equal standing in academic research due to the intricacy of showing proof and repeatability. Traditionally predictive modelling has mostly been confined to linear regression modelling, and to some degree to nonlinear time series e.g. price forecasting of instruments on a market. (Delen & Demirkan 2013)

Predictive analytics encompasses all traditional regression techniques, but also includes other types of analysis, e.g. Social Network Analysis (Borgatti 2009) or Sentiment Analysis (Liu 2010). The type of predictive question asked can be of either a descriptive or prescriptive nature, but focuses on what will occur in the future. The basis of every answer is a value, sometimes referred to as a predictor, which describes a forthcoming event. The predictor can e.g. be the potential of someone making a purchase on a web site depending on an earlier shopping pattern. Prescriptive analytics techniques, on the other hand, can use this probability in order to set a price that maximises company revenue in total, by weighing in how other subjects have behaved. The travel industry (airlines and hotels) is perhaps best known for employing these types of techniques, which, albeit still being relatively naïve, are used for setting a customer specific price for the transaction (Taylor 2012).

Following is an overall classification of the primary analytical methods. They are also exemplified by how analytics connects to the social/technical environment regulated by the GDPR. As earlier stated, there are three main categories of analytical methods; descriptive, predictive, and prescriptive (normative).

Depending on the analytical task (what we want to know about a data subject), we can use methods from these categories either individually or in combination. The underlying machine learning methods may often be related or similar for all three categories, but the categories below are described per function of objective.

Descriptive Analytics – Understanding events by mining historical data, to look for the reasons behind past success or failure (Oracle 2012). Reducing dimensionality and/or compressing data by grouping actors, events, or data points together. Identifying relationships in data and visualising these for a human operator. A common service utilising descriptive analytics is a traditional search engine.

Predictive Analytics – Finding probable future outcomes by turning data into actionable information (IBM 2010). Capturing patterns and relationships in past data that can be used to forecast a future event by some probability. The assumption made is that past patterns will reoccur in a similar format in the future. An example of predictive analytics is the use of profiling in the travel industry for direct marketing.

Prescriptive Analytics – An ability to synthesise optimal decisions from big data, context rules (e.g. business rules), and machine learning, determining decision options that are as good as possible from data, rules, and modelling. In its original form, prescriptive analytics did not necessarily include forecasts, e.g. solving a scheduling problem according to a defined goal function (Evans and Lindner 2012). Currently, more advanced forms may involve both predictive functions and objective reinforcement learning. Examples include both optimisation and simulation of problems that can be defined by system rules, which are established either manually or derived automatically. A digital personal assistant could be classified as using prescriptive answers when guiding the individual.

2.2. Application of Analytics in Industry

Operations research focus on employing mathematical techniques, such as mathematical modeling, statistical analysis, and optimisation. Operations research arrives at optimal or near-optimal solutions to complex decision-making problems[12]. Analytics may use, but are not limited to, operations research methods. However, the main difference between the two is that analytics focuses on the scientific process of transforming data into insight for making better decisions[13]. This implies that analytics can be seen as a holistic approach for processing data,

[12] See https://www.informs.org/About-INFORMS/What-is-Operations-Research
[13] See https://www.informs.org/About-INFORMS/What-is-Analytics

performing analysis, asking questions that provide insight, and finally considering the objective of decisions that lead to actions (Liberatore and Luo 2010).

The terms big data analytics or data analytics (as a more general term) have today been adopted by industry and academia to describe the integrated use of advanced mathematical modelling, big data, cloud computing, service-oriented architectures, and decision support systems (Delen & Demirkan 2013). Analytics is used to describe the process of extracting relevant decisions from data (Davenport 2006). The potential of analytics often extends beyond the use of historical data into a real-time setting, thereby allowing for an instant as well as automatic interaction with the consumer (MacMillan 2010). Analytics has also become a general term for describing data driven efforts to gain insights into a general process or situation without a direct business decision interest. Traditionally academia has used operations research as the term defining the interaction of data, mathematical modeling, and information technology in a business setting. In the following sections, we go through some of the important historical research branches leading up to the use of analytics in companies.

In section 5.1 in this thesis we detail an implemented generalisable and scalable architecture for processing temporally structured data. The architecture enables the application of real-time analytics and the use of historical data for training models. The development work started in 2012, and by 2013 open-source tools such as Hadoop were available to perform machine learning based analytics on historical data, as detailed in section 5.2. In 2017, we can consider that most multinational enterprises are actively investing in developing the ability to analyse each transaction in near real-time for each data subject, be it a person or a product. Analytics opens up great possibilities for companies with access to massive amounts of data on their users and products. Analytics will e.g. allow companies to customise their product assortment to better suit certain customer segments. Netflix, a provider of on-demand Internet streaming media, reportedly bought the rights to the political/adult-content drama series House of Cards after analysing the viewing habits of their customers and finding they correlated with the themes for the storyline of House of Cards (Davenport 2013). The analytical methods employed have a descriptive nature, i.e. finding the customer preferences from historical data. The way Netflix made use of the understanding can be considered a prescriptive service, since once the TV-series was made, Netflix were able to suggest to particular households a solution that viewers were unknowingly yearning for. This serves as a good example of the difference between utilised analytical methods and intelligent service design strategies.

One of the better-known early examples of the use of predictive analytics described in media was how the US-based retailing chain Target deduced women were pregnant by analysing a change in shopping behaviour. When customers using loyalty cards went from buying scented body lotion to non-scented, Target tracked

this information, classified them as potentially pregnant, and started marketing products that were needed in early pregnancy to them. The insights behind the conclusion, that there potentially was a pregnant woman in the household of the loyalty cardholder, was in this case derived manually (Duhigg 2012). However, there is nothing holding back the automation of such insights and decisions as long as enough data exists and a sufficiently reliable predictor can be trained. Either supervised or unsupervised training methods can be applied depending on the required output (Enkvist & Westerlund 2013).

The two examples of Target and Netflix both show how information about users can be synthesised. Pregnancy in this case can be seen as very sensitive information (cf. Wong 2007). Even if Target did not collect health information *per se*, the synthesis of such information, for the purpose of using it in a commercial setting should be interpreted as sensitive information. A similar argument can be made from the ECJs statement in the Lindqvist Case (C-101-01) where the court held that in the light of the purpose of the Directive, the expression "data concerning health" used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual.

The Target example shows that whole households can be purposely profiled for revealing very sensitive personal data about someone in the household who does not necessarily want to share such information. The Netflix example on the other hand reveals that data can improve the user experience for their customers. However the insights may still not be suitable for sharing with the whole household. We can note that the service provider in the two examples may be unable determine a specific individual in the household to aim at. The inability to determine the exact physical data subject in a household and the risk of an anonymity breach by suggesting a revelatory sensitive insight to another individual in the same household ought to make such service insights in Europe questionable without gaining explicit consent from the data subject.

2.3. Management Support Systems

In a computerised setting, the use of information systems to automate the processing of data into (a) decision(s) in an enterprise is often performed by so-called management support systems (MSS) (Aaronson et al. 2005). A management support system is based on the principles of decision theory. Decision theory states that an optimal solution can be determined given the values, uncertainties and other relevant matters for a given decision. Decision theory thereby focuses on finding the optimal solution for a given problem. The different types in the classification of analytics, provided in section 2.1, has its roots in decision theory. Bell et al. (1988) defines decision-making as either descriptive, normative, or prescriptive interactions. There are two main types of MSS that have a relevance for

understanding the GDPR; decision support systems (Sprague 1987) and expert systems (Feigenbaum et al. 1993). To condense their difference, expert systems can be seen as automated processing systems, while decision support systems require interaction with a human. We should however note that the definition of the latter is more ambiguous, as processing of data leading up to a proposition can also be automated in a way that hides the influence of any underlying parameters. This can be problematic in case the modelling infers any discriminatory practices. Both types of MSS tend to use similar methods, while the systematisation question and level of system autonomy may differ.

2.3.1. Decision Support Systems and Business Intelligence

The analysis roots in decision support systems (DSS) and business intelligence can be traced to the statistical (descriptive) methods developed during the 1970s and data mining techniques developed in the 1980s (Chen et al. 2012). Business intelligence that utilise a DSS has largely focused on business performance metrics/indicators using balanced scorecards. Chen et al. (2012) classified these types of systems as the first version of a data-centric approach to management. Data management and warehousing is considered the foundation of version 1.0. They state that the use of scorecards and the extended dashboards help analyse and visualise a variety of performance metrics. The data structures used in version 1.0 are often relational, meaning that data is considered pre-structured and includes important metadata in the relations constructed.

The following version 2.0, in Chen's et al. (2012) maturity model, focuses on integrating internal business data with user-generated content. This type of user-generated content can e.g. take the form of social interactions in web-based systems, such as forums or product reviews. User-generated data are often regarded to be of an unstructured nature. Davenport (2013) extends the definition to focus on the concept of big data as the key driver. He identifies the need for scalable tools that can handle user-generated big data in order to deliver business relevant insights/decisions at a moment's notice.

The third version (3.0) is broadly considered to be about data-enriched offerings were industrial companies, not just the online or information business, become digitalised (Davenport 2013). To enable such a development, companies will want to start generating data on any physical process in their reach. For example, an automobile manufacturer is no longer satisfied by receiving data once a year (or according to the service interval) when the car is brought in for the annual inspection to the local service centre. Rather, the manufacturer wants to monitor continuously any of the numerous sensors in the automobile. Still, data-enriched offerings go beyond monitoring. Manufacturers for example in the automobile industry are currently competing on who can build the safest driver assistance system, that makes use of sensor data in real-time. The data collection and modelling

approach chosen is to use data from other automobiles as well, in order to improve the ability of the assistance system. The assistance system can then be automatically updated when needed over a mobile connection. Tesla, the manufacturer who arguably has gone furthest in the marketing of their autonomous driving assistance system (Autopilot), has, according to media reports, logged over 160 million km with the Autopilot active (Simonite 2016). The separation between a DSS and an expert system in this example can be defined as the latter being implemented as a fully automated autopilot, were the human goes from being a driver to becoming a passenger. To be compliant, a decision support system which handles personal data and creates propositions that are acted on by a human operator, should, when requested by the data subject, also be able to determine what parameters influenced the proposition. We here consider recommender systems as similar to a DSS, as they also do not act on decisions autonomously either. However, considering that recommender systems often present options to a data subject based on personal data, such a system should also adhere to the regulation.

2.3.2. Expert Systems

In addition to being data driven, expert systems are knowledge driven. The designer of an expert system should understand the system dynamics so well as to be able to automate decision-making. Traditionally we have seen this implemented through two different branches: applied artificial intelligence (i.e. machine learning) (Gallant 1993) and rule-based systems. Decision-making in rule-based systems has shown that fuzzy logic methods enable decision-making also with estimated values, thereby significantly extending the real-world application of rule-based solutions (Carlsson and Fullér 1996). In systems based on machine learning this often includes some sort of derived intelligence in terms of reasoning over an objective. Game theoretic-based solutions have been proposed for solving the reasoning problem (for a network security application see Hu et al. 2017). Game theory examines the possibility of conflicting or optimal solutions to interrelated problems. Hence, game theory focuses more on simulating scenarios. An optimal solution would not be defined as the best solution, but rather as a good enough solution or as a better solution than what is currently available. Recent research into reinforcement learning (see e.g. Mnih et al. 2016) focuses on understanding the mechanisms in automatically determining multiple objectives where the relative importance of the objectives are not known a priori (Mossalam et al. 2016). A system able to deal with multiple objectives offers autonomous agents a more human-like reasoning ability. An autonomously driving car as in the example above, may have to choose between avoiding hitting an obstacle in the middle of the road or manoeuvring the car into a ditch. If the obstacle detected is considered an animal the response may be different than if a human is detected. If the probability is sufficiently high of the passenger

being fatally injured in the manoeuvre, then the rationality for the decision becomes circular and more difficult to solve.

This latter definition of expert systems as autonomous agents, particularly with objectives derived autonomously, has a compliance implication for the GDPR as well (cf. RQ1). First, the use of automated processing of personal data, as later discussed, is limited. Second, agents that possess autonomously derived knowledge may not be under the explicit control of a controller, thereby limiting their potential use for personal data. A third implication may be related to the definition of personal data, as this is based on a direct or indirect ability of the controller or processor to identify a natural person. Defining an expert system as fully autonomous, incl. automated data processing and decision-making, may make it possible to argue that the legal person behind the agent is not in a position to determine the physical identity of the data subject, hence limiting the application of the GDPR.

2.4. Machine Learning

An important enabler for intelligent assistant systems are the models that act as pattern recognition algorithms. These algorithms often go under the name machine learning models or deep learning models. A model learns its original pattern recognition behaviour from historical data. The desired behaviour for the model can be defined by providing a target variable for each input vector. The model will then adjust itself to produce an output response corresponding to both input data and the target variable. Such model training is termed supervised learning. The opposite of supervised learning is unsupervised learning. For unsupervised learning, a target function is not provided for the input data given to the model. Rather, in unsupervised learning the model often strives to categorise input vectors into clusters of related data.

An example of a supervised learning model is the artificial neural network (also referred to as a neural network). The development of the neural network has its history in the Perceptron developed in the 1960's. A neural network has an input layer, at least one hidden layer, and an output layer. The learning method then attempts to find a non-linear mapping of the input vector into a high-dimensional feature space (hidden layer). Connecting the high-dimensional feature space to an output layer can then be performed through linear mapping (Haykin 2009). There are several types of supervised learning models, such as the Recurrent Neural Network, Support Vector Machine or the Extreme Learning Machine. The learning problems solved with supervised learning are either a regression or a classification. In a regression, the model attempts to reconstruct a continuous function, provided to the model as the predictor variable, while the classification entails a mapping of inputs to (a) discrete (non-continuous) output(s).

Unsupervised learning has its roots in information reduction techniques through the use of associative memory. An early example of such a model is the Self-Organising Map (Kohonen 1981). The self-organising map finds complex relationships based on input features and maps these into a given number of clusters. An unsupervised learning technique used for training a self-organising map model is competitive learning. Competitive learning works by specialisation of neurons in the model. To distinguish two input vectors their quantified distance is measured and compared, e.g. using the Euclidean or Hamming distance. In unsupervised learning, corrections are not performed through an external process, as often the expected solution is not known. Conversely, the clustering output may contain clusters that represent information in an unsolicited manner (cf. RQ1). This may create the predicament that clusters are created based on personal data, which contain special categories of personal data, such as religion, race, sexuality, or health. Now the processor and/or controller may or may not know this as a fact, but this has a clear implication on the creation of profiles on data subjects.

Although here described as two separate learning methods, in reality, these methods are often combined or mixed in the analytics workflow. The described models are often referred to as shallow learners, as their accuracy in tasks based on complex data, such as image or speech recognition, is usually much worse than what a human being can perform. Shallow learners focus mainly on a one layer mapping process between input and output. In more complex deep learning models results are often on par with, if not exceeding, human recognition. Deep learning models, such as a deep convolutional neural network, often employs both unsupervised learning and supervised learning techniques in combination. The unsupervised learning phase tends to perform feature engineering, while the supervised phase defines the model target. In 2012, Krizhevsky et al. won the ImageNet competition by reducing the classification error from the runner-up's 26% to 15%. For this task, he employed a deep convolutional neural network. An important insight gained from deep learning models is that these types often perform better in feature engineering than a human being. Deep learning has also received critique for being computationally heavy, compared to shallow learners. Deep learning typically requires massive datasets to be used for properly training the models (Chen and Lin 2014). Essentially the more data that exists the better the models' end result tends to be. This demand for data is in stark contrast with the GDPR requirements of data minimisation and the privacy-by-design methodology.

Another critique towards deep learning is their sensitivity to tampering. An adversarial attack manipulating the dataset used for training the model could lead to undesirable results. Research has shown that for image classification tasks, manipulating an image with for a human undetectable noise, means that the image is no longer classified correctly (Goodfellow et al. 2015). Machine learning techniques are also susceptible to stereotyping and bias due to the training dataset

(Miltenburg 2016; Danks and London 2017). For instance, when Microsoft's Twitter chatbot Tay was introduced to the public it developed, through a symbiotic interaction, a behaviour considered racist (Neff and Nagy 2016). The GDPR requires companies to ensure the integrity of a data subject's personal data. The sensitivity of machine learning models in regards to noise in training data (incl. adversarial attacks on training data) and sensitivity to symbiotic stereotyping may, inter alia, make the launch of personal digital assistants more difficult. To generalise, these two presented examples show the frailty of artificial intelligence technology imposed on an interconnected society that value digital privacy (cf. RQ1). Developing intelligent technology is not only a question of innovating, but one also needs to consider being compliant with a long-reaching GDPR.

2.5. Scalable Cloud Computing Architectures

Cloud computing can be described as a utility service in which computers, storage, computing power, or software, is rented virtually over the Internet. The rapid proliferation of 'X as a Service' (XaaS) type services in the cloud space have to a degree contributed to the commoditisation of complex information technology infrastructures. As an example, today anyone can create and run a supercomputer (i.e. thousands of linked computers) for a minimal cost when needed, without having to deal with the setup of the information technology infrastructure or develop the software needed. The 'X' in 'X as a Service' can be any type of digital service, which can be defined by the ability of scalability. Scalability refers to both a certain standardisation of service as well as to a microservice or modularity based software architecture. To scale horizontally means to add more hardware while achieving a near linear increase in processing ability. The driving force behind such software designs has been the Service Oriented Architecture (SOA) approach (SOA Manifesto), which has become an industry de-facto standard for building cloud based, loosely-coupled "X as a Service" enabled data sharing software modules.

The evolution of SOA has transitioned cloud architectures towards stand-alone microservices that improve the ability to both scale and standardise services even further. Lewis and Fowler (2014) compare the microservice style to the traditional monolithic style to better explain the differences. The monolithic application is built as a single unit, often as a single logical executable that runs in a single thread. Any changes incurred on the system involves building and deploying a new version of the complete system. To horizontally scale the monolith can be done by running many instances behind a load-balancer. The monolith instances then become activated based on requests coming into the load-balancer. The more requests coming in, the more instances are then replicated over more server hardware. However, once the monolith grows, maintaining a modular structure of the code, updating a small part of the code, or testing out new features on a subset of users through continuous user testing, can become frustrating. To implement continuous

integration and continuous user testing, both an enhanced software architecture, such as the microservice style, and new production tools that support the creation of native cloud applications are needed. A microservice achieves componentisation via a service that exists as an out-of-process component, which communicates with other services through a mechanism such as a web service request, or remote procedure call (Lewis and Fowler 2014). Microservices aim to be as decoupled and as cohesive as possible and have their own domain logic. Therefore, a microservice does not aim to reuse code, but rather is designed for code replacement.

The ability to perform analytics using machine learning based models can be implemented using in-house developed, proprietary, or open-source software. If the intended use requires massive processing power, i.e. individual model training or transfer learning per user, then this will require a massively scalable processing architecture. The use of microservice frameworks can support the personalisation of services. However, our findings are that scalable processing architectures can be implemented efficiently through a generalised worker/master node architecture, were the master-node performs a type of scheduling duty (cf. RQ2.1).

In section 3.1, the construction of an in-house developed scalable processing architecture is presented. Section 3.2, presents an algorithm implementation on Hadoop, an open-source based solution for storing and processing big data. The choice of solution may be project dependant; however, a finding from the presented work is that the complexity of such a processing architecture opens the software to an increasing number of network security attack vectors. The use of well-tested proprietary or open-source software may mitigate this risk; however, the use of well-known software also requires a continuously updated software environment. The challenge of employing current open-source big data solutions is that they include a great number of bindings to various other software libraries, which may be demanding to keep up-to-date. As a response to RQ2 and RQ2.1, in section 3.1 some high-level security considerations to deepen the understanding of the complexities involved in creating scalable systems are also provided.

2.6. Big Data Software Design

Big data is often explained through the four data describing V-attributes: volume, variety, velocity, and veracity (accuracy)[14] [15]. A fifth attribute, value, was added later to explain the value creation process in the organisation. Value is thus considered to arise from the ability to analyse data in order to develop actionable information (Kaisler et al. 2013). As previously stated, designing software that is able to handle big data requires a horizontally scalable system that usually resides in the cloud.

[14] Laney (2001) introduced the first 3 V's and IBM added later the fourth V – veracity. Other attributes has also been proposed, such as value, complexity, and unstructuredness.
[15] For an in-depth discussion see De Mauro et al. (2015).

Considering the process model for analytics presented in section 2.2 and the data centric V-attributes, an overview of programming related issues and considerations that often arise when designing big data analytics software are here presented (see Table 2). This section connects the technically focused sections 2.4 and 2.5, to a design-focused, and thereby a higher abstraction point of view, as is represented in the other sections in this chapter.

As big data grows in volume, storage capacity on a single node is no longer enough, and may require a distributed multi-node solution. Processing power during the analysis phase may likely require a similarly distributed multi-node solution (see section 3.1 and 3.2).

Table 2 - Reference model for typical Big Data Analytics software design issues

	Data	Analysis	Insight	Action
Volume	Storage capacity	Processing power		
Variety	Integration of data sources	Data transformation	Inputs representative of problem	
Velocity	Throughput	Latency		Time to react
Veracity	Correctness and completeness	Outliers and modelling choices	Do we ask correct questions	Trust in decision and risk management.

Great variation in the type of data generators often require extensive integration of data sources. A common design architecture is to create a master data source that any consequent analysis endeavour can then employ. This may improve integrity and thereby minimise the risk of using erroneous data. Using a master data source may also make it easier to utilise disparate data sources, but to succeed master data may require a massive governance organisation. Data of different types often involve data transformations dependent on the analysis context and models utilised. During the insight stage, effort must be given to determine if data types are representative of the question at hand.

A relatively new problem in academic settings is how to deal with data streams. Velocity has traditionally not been a research problem for operations research, as the data primarily used has been at rest. Data throughput is often measured as the data amount that can be stored per a given time in a database, but within real-time analytics this data must also reach processing nodes. Once processing nodes completes the analysis, latency needs to be smaller than the throughput frequency (rate measured in transaction/time interval). If latency is higher than the throughput frequency it leads to lags in the system or the input resolution can be reduced, e.g. through compression.

The veracity of a management support system is naturally of paramount importance. However, in big data analytics this may rather be expressed as a probability statement. If the chance to be correct is greater than being wrong, it might be enough to take a certain decision, particularly if the downside of being wrong is small and the benefits of being right is comparatively greater. When it comes to the quality of big data we have to assume that input data has a certain level of correctness and completeness, but the great number of samples may make up for certain inconsistencies in quality. Pre-processing of data is often the most time consuming step in creating analytics software and may sometimes require estimation of missing values and correction of input errors[16].

During analysis, veracity needs to be studied both in regards to the modeled data and to the type of model chosen. To achieve true insight we need to ask the correct questions. Any action developed based on this insight needs to be either logically or factually sound. In performing real-time analytics, we measure validity continuously and not only during training or testing. Depending on the area and solution, we may also have to perform risk management continuously.

The development of big data analytics enabled software solutions has mostly been driven by the existence of massive unstructured datasets. Analytical systems have recently received a great deal of attention from academics, open-source community, as well as industry (see e.g. Begoli 2012; Fox 2012; Valvåg et al. 2013). In addition, standardisation steps in big data analytics have been taken (Ghazal 2013). An initial seminal paper published by two Google researchers, Dean and Ghemawat (2004), laid out a software architecture for data processing called MapReduce. The paper discussed an approach for introducing an abstraction to deal with complexities arising from the need to massively parallelise a processing task over hundreds or thousands of nodes. The researchers realised that many of the processing tasks involved in constructing a search engine could be summarised to two main operations. The first operation is a mapping of logical data (relevant records from the input) to a key/value pair. Then a reduce operation, were each value that shares a key is combined, is performed. The approach is influenced by various functional programming languages that have a similar map and reduce approach for single node processing. The benefit with the MapReduce programming model then becomes that it decomposes data into smaller pieces, which are then processed on the network hosts in which they reside, instead of moving the data pieces to other network nodes for processing. This type of programming model can be considered one of the fundamental technical principles for implementing scalability in data processing. The programming model is particularly suited for processing unstructured or semi-unstructured data, where content lacks a strict

[16] For an approach to estimate missing data see e.g. Sovilj et al. (2016).

schema defining the data model; often suggesting that input data can be decomposed without a negative effect on the processing output.

In the case of structured data, section 5.1. presents an alternative cloud computing architecture that allows horizontal scaling using spatio-temporal structured data (Westerlund et al. 2014). One of the challenges using spatio-temporal structured data is when data needs to be processed both in batch (at-rest) and in real-time (stream data). Dependencies introduced early on in the process workflow need to be accounted for in process stages later on. The inspiration for the software architecture came from grid computing, but through utilising cloud computing resources. When designing our architecture, we defined a design requirement that any processing (both batch and real-time) had to be performed using a unified processing architecture. During the model training workflow, we used data at rest, while in prediction mode we could use both at rest and real-time. Real-time data can have different definitions depending on the context. In a cloud environment, we often define real-time data as either a segment or an event. The difference is that a segment stores a small data buffer of a certain size before it is sent to processing. The size can be determined based on a time limit or amount of data. On the other hand, event driven often infers that data are sent to processing as soon as the system receives the data. There are certain technical reasons for using a buffer, such as reducing overheads and improving latency. For this reason, many of the big data analytical tools such as Hadoop and Spark mostly use a segment based processing model. Since our design goal was to design an event-driven model, we chose a star topology as a network architecture, instead of the mesh-driven network topology used in most other big data tools. The star topology binds the data model to the worker node while active, which may have a detrimental effect on node reuse times in truly massive environments. This occurs because a new data model must be loaded each time the node needs to be repurposed. The star-topology on the other hand also allows a dedicated processing environment, were a designated node can with small overhead, continuously listen for new events in real-time, and thereby avoid some of the latency issues that might arise otherwise. In a real-time processing environment, our implementation considers the worker node as the solitary handler of a specific responsibility.

One added benefit from our architecture is that we can isolate data per processing node. This can be considered to provide the system controller with a more fine-grained access control to potentially personal or sensitive data. The fine-grained access control can be applied to both user access and to model access. Model access here refers to models that are certified being ethically designed and approved. This discussion and the response to RQ2 and RQ2.1, continues in chapter 5.

2.7. Platform Economy

The Internet was started on what can be considered idealistic goals such as openness and free services. The rise of the global tech behemoths over the last decade may have changed these ideals and the nature of the Internet permanently. The platform economy as a theory for explaining how companies employ the network effect to their competitive advantage, has gained wide academic support (Hagiu and Altman 2017). The role of platforms in building the Internet enterprise is also becoming increasingly evident. Platforms have been instrumental in changing consumer behavior and are also opening the way for radical changes in how work and value creation is being organised (Kenney and Zysman 2016). They can change industries that have been closed and sometimes heavily regulated, for example the telecommunication industry as later discussed. The early work of Cusumano and Gawer (2002) showed a clear tendency that successful technology companies often acted in symbiosis on several levels with other successful companies. In particular, they highlight the interconnectedness between companies such as Microsoft (software), Intel (hardware), and Cisco (network) in creating the PC-platform and how each company supports their own complementors, "companies that make ancillary products that expand the platform's market". Rochet and Tirole (2003) emphasise the price discovery process for multi-sided markets and find two different price structure approaches. The early game console platform market employed a model financed by the seller side (game developers), to be contrasted by the opposite model that is consumer financed in the PC-market. Parker et al. (2016) highlight a third alternative price structure, whereby consumer generated data is processed and then sold forward to third parties (e.g. to data stores or marketers) in a refined form. Gawer and Cusumano (2014) consider there is strong evidence pointing to that the platform tends to shape industries through the interaction between companies and users.

Parker et al. (2016) defined this interaction between users (both individuals and companies) on the digital platform as a transaction. When a new platform market can be introduced to an industry, it will likely open the industry to the threat of new competitors. Kenney and Zysman (2016) has argued that platforms will become a core organising principle for a new economy. The platform economy is often defined as a result of a market that is created through the facilitation of transactions between market participants. Emphasising the difference to a technological definition, which focuses on the platform as an intermediary fabric for delivering various types of data. The price structure Parker et al. (2016) described has become the standard model for offering "free services", where consumer generated data are processed and then sold forward to third parties in a refined form as payment for the use of the platform. The incentives for establishing the platform then become closely related to the ability of utilising massive computing resources for the purpose

of gaining an understanding (insight) of the users and then conveying this information to other market participants willing to compensate the platform owner for gaining access to this user base.

As defined in section 2.2 the ability of gaining insight through analytics can be classified into three main categories. The analytics categories can be connected to the platform through the type of insight they offer and what monetary value/return a company can hope to achieve by using them. Descriptive insight may offer the smallest monetary value, while prescriptive insight has the potential to change customer behaviour and is thus the most coveted form. Predictive insights can certainly also influence customer behaviour, but it is more focused on earlier behaviour than creating new experiences. If the aim of the future digital platform is to create monetary value for its owner, then it will likely be driven towards offering prescriptive insights.

The challenge of creating prescriptive insights is that the data needed should encompass the life of the individual, and not only in relation to the current event/process that is being evaluated. Providing someone with complete access to all data regarding the individual extends the data protection question beyond that of lawful processing to the construction of systems with guaranteed data security, something that today may sound like a utopia. Still, some may argue that as long as the processing is done in the best interest of the user of a "free service", then it causes no harm. Related to this is the discussion around who owns user-submitted and/or created data through profiling (the encapsulated model insight). Platform owners, as will later be shown, have made very few concessions regarding ownership or ability to process data. As the incentives until now have only been geared towards processing any data stored on the platform, many, and among them the European Commission, have considered that self-regulation in the sector is not enough, and thus anyone found violating the GDPR face considerable fines, up to €20 million or 4% of global annual turnover, whichever is the greater. In response to RQ3 we will continue the platform discussion in chapter 6 and 7.

2.8. Summary

The aim of digital platform companies is to create an interaction between users and users, and users and customers (companies). This interaction leads to an accumulation of data that can be transformed into insights through the use of analytics. We here refer to the term analytics as a technical synonym for processing used in the legal text of the GDPR. Analytics may include process steps from storing, extracting, transforming, and loading, to model training, validation, execution, and maintenance. In the construction of intelligent services, analytics also has a great importance for the human-computer interaction. In section 2.3, the connection between management support systems and the GDPR is highlighted (cf. RQ1). The potential use of fully automated decision-making expert systems is limited by the

regulation. In addition, machine learning algorithms, particularly those trained with unsupervised learning or reinforcement learning methods, may also expose the controller (owner) to additional GDPR compliance risks. The difficulty in determining the behaviour of these types of algorithms should not be considered leading to a lessened accountability.

The practical use of analytical systems typically require them to be scalable. One important factor to become scalable is the ability to grow the processing environment when required, and shrink the environment when resources are no longer needed. To achieve this elasticity, a public cloud is often used. This solution opens the system to new network and data security threats that need to be mitigated (cf. RQ2.1).

The thesis defines the aim of analytical services as *descriptive*, *predictive*, or *prescriptive*. Prescriptive services have the potential to change consumer behaviour, thereby offering great revenue enhancing possibilities to companies that are able to build such services. Because of this, companies will ultimately pursue the creation of prescriptive services. To create insightful prescriptive services, companies will need to access as much data as possible regarding a user. Introducing IoT into the home will in time digitise any personal experience occurring inside the walls of private property. The GDPR highlights the importance of data minimisation and privacy-by-design, the clash between the technological and legal views are obvious. Regulating digital platforms is certainly important if we want to remain private in our own homes. However, anticipating the challenges is very difficult (cf. RQ3).

Research in network security is progressing, but immense practical challenges in securing information systems still remain. The use of open-source software has likely raised the bar for security, but it has also introduced new challenges (cf. RQ2). Broadly speaking, perhaps an overreliance on built in software security in open-source software exist today. An increasing amount of software bindings and the introduction of lightweight microservices, which can easily be deployed by almost anyone in the organisation, may reduce that security barrier going forward.

Why should it be that just when technology is most encouraging of creativity, the law should be most restrictive?

—Lawrence Lessig

3. Data Protection Legislation

The following chapter introduces some important legal concepts regarding the Data Protection legislation. The regulation includes many amendments of the Data Protection Directive (95/46/EC) and therefore the directive is briefly introduced. The Regulation also includes completely new legislation to ensure modern data protection while still maintaining a strong business environment in a unified Europe. The reader should note that the regulation has undergone a revision process, which consequently have introduced changes. The GDPR text used is the consolidated version referred to as (GDPR 2016)[17], signifying that some additional insertions (e.g. recitals) and numbering changes has occurred in the adopted text.

3.1. EU Legal Acts Relevant to the Digital Landscape

As the digital landscape has matured, the Regulator has introduced a set of legal acts that may affect a service or platform provider. These acts can be categorised into two main groups; sectorial and wide-ranging. An example of a sectorial act in the EU can be found in the health care sector[18]. Wide-ranging acts, such as the GDPR, establish a common practise for operating standards and what can be considered a minimum of respect for the rights of the weaker party. The raison d'être of EU law has been to bring together the economies of the Member States. For this purpose, the EU Regulator has different instruments at his disposal. In this thesis, primary sources such as regulations and directives are considered. Other primary sources referenced are previous court decisions and motivations behind a decision. Secondary sources that are relevant for the technology field are working groups, standards, and communiques that aim to find common practise and a measure of self-governance. Other secondary sources referenced are the work of legal scholars.

The debate over whether to have a general data protection legislation or a specific abuse-based legislation, was mostly conducted during the introduction of the data protection directive in the 1990's, but still continued in some countries until the early 2000's[19]. This coincided with the introduction of the Internet to the general population. At the time the Member States demanded that they be able to specify

[17] European Parliament and the Council of the European Union, Regulation (EU) No XXX/2016 of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 15039/15, consolidated text of the General Data Protection Regulation as an outcome of the final trilogue on 15 December 2015. Can be accessed http://data.consilium.europa.eu/doc/document/ST-15039-2015-INIT/en/pdf last accessed 12.08.2017.

[18] EU Regulation on Community statistics on public health and health and safety at work (EC 1338/2008)

[19] For a historical perspective focusing on the Swedish experience, see Öman, S. (2004).

the specific conditions governing the lawfulness of data processing in their national law. One reason for this may have been that the EU Charter of Fundamental Rights only became legally binding in 2009, only after this all Member States guaranteed their citizens personal data protection as a fundamental right (Charter (2000/C 364/01) art. 8). In passing the Directive, the EU Parliament called for the Member States to strive to improve the protection currently provided by their national legislations. The data protection directive was introduced for dealing with an increase in international trade among EC countries and the consequent transfer of personal data. However, already then it was foreseen that a directive might become problematic, as the national legislation differences would have an effect on the movement of data within the Community, and thus leading to disputes and ambiguity over whose legislation should be abided by[20].

Some countries (e.g. Sweden (Datalagen SFS 1973:289)) had a long tradition of legislation dealing with automated processing. Efforts considered prior to the Directive had also been performed at OECD in 1980 to create international guidelines. However, without an enforcement mechanism they were considered mostly ineffective (Boyd 2006). In 1995, the European Council and Parliament adopted the directive with a strong link to the United Nation declaration of human rights (privacy of correspondence)[21] and the establishment and functioning of the internal market (Boyd 2006).[22] Member States were required to enact national legislation by 1998.

3.1.1. Other legal acts influencing the digital landscape

In addition to the general data protection legislation, other relevant acts that influence the digital landscape exist. As they further the understanding of the Regulators intention in connection to security and tracking, their scope is shortly summarised below.

The Directive on privacy and electronic communications (2002/58/EC), also known as the e-Privacy Directive, mainly concerns the electronic communication networks regulating confidentiality and treatment of traffic data. This directive was later amended by what became known as the Cookie directive (2009/136) that introduces changes to how tracking information is collected. At the time of writing, the EU Commission has given a proposal for an e-Privacy replacement, this time a regulation. The replacement regulation is considered needed to handle new types of

[20] See the data protection directive, recital 9.

[21] Universal Declaration of Human Rights, G.A. Res. 217A, U.N. GAOR, 3rd Sess., Part I, at 71, U.N. Doc A/810 (1948). Article 12 states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."

[22] For a historical and comparative study between USA and EU regarding privacy from a legal standpoint, see Boyd (2006)

communication applications and corresponding meta-data, simplify tracking consent, protection against SPAM, unifying the national adoption, and a harmonisation in regards to the GDPR[23].

The Directive on Network and Information Security (2016/1148) applies primarily to defined infrastructure (operators of essential services) and certain digital service providers. The intention of NIS is that it should not place additional burden on small and medium sized enterprises but rather be a recommendation for dealing with security and security incidents. It should be noted that the handling of security incidents involving personal data or sector-specific data are further specified in, for example, the GDPR. Incidents are defined as any event having an actual adverse effect on the security of network and information systems. Enterprises that fall within the definition of the directive and thus must fulfil its obligations are operators of essential services, such as energy, water, transport, banking, financial market infrastructures, healthcare, and digital infrastructure. Some of the requirements defined under NIS are preventing risks through appropriate technical and organisational measures, ensuring IT security appropriate to the risks, and handling incidents to minimise impact. (Pulkkis et al. 2018)

3.2. Certain Relevant General Data Protection Definitions

The Regulation has certain limitations in applicability. To understand these limitations, definitions of some central terms are provided in the sub-sections below.

3.2.1. Personal Data

The definition of personal data is highly important because it states whether the data protection legislation is applicable or not. Personal data is characterised as only such data that can be linked to a natural person (i.e. an individual's physical presence). Any other type of data is not relevant from a legal perspective when it comes to the GDPR. Accordingly, the GDPR should not be considered to provide protection for legal persons such as companies.

The regulation defines personal data as any information related to identifying a data subject. The physical person thus becomes a data subject if data related to the natural person is processed. Personal data thus receives a wide definition in the regulation:

> 'personal data' means any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors

[23] See EU Commission communication, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation last accessed 09.08.2017.

> specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. (GDPR 2016, art. 4(1))

An earlier version of the GDPR (2012/0011 (COD)) defined it differently, as "*means reasonably likely to be used by the controller or by any other natural or legal person*" to identify the data subject. Both definitions raise several questions about what type of data or information, as stated in the definition, is classified as such. The design implications due to these issues are discussed in section 4.1.

There are two sensitivity classes defined for personal data; normal and special categories. Special categories of personal data include, inter alia, data related to criminal convictions and offences that may only be processed under the control of an official authority or when the processing is authorised by Union law or Member State law. A register with data on criminals and their corresponding convictions has a specific requirement that it may only be kept under the control of an official authority. Other special category definitions are genetic data, biometric data, and data concerning health.

Genetic data represents data relating to the characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, particularly resulting from an analysis of a biological sample from the individual in question (GDPR 2016, art. 4(10)).

Biometric data denotes any data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual (GDPR 2016, art. 4(11)). Examples are facial images or dactyloscopic (fingerprint) data. It is however important to understand that an image of a face is by itself not considered biometric data. Facial images will only be covered by the definition of biometric data when being processed through specific technical means allowing the unique identification or authentication of an individual (GDPR 2016, recital 41).

Data concerning health signifies data related to the physical or mental health of an individual, also including the provision of health care services, which reveal information about his or her health status.

In addition to the described special categories of personal data we find racial or ethnic origin, political opinions, religious or philosophical beliefs, and trade-union membership (GDPR 2016, art. 9(1)). Considering a use case when personal data needs to be archived, then the recommended approach, where possible, is to first protect data through pseudonymisation. Pseudonymisation of personal data entails the transformation of data so it can no longer be attributed to a specific data subject without the use of additional information. A possible key that can be used to transform data back to its original form ought to be kept separately and subjected to technical and organisational measures to ensure non-attribution to an identified or identifiable person (GDPR 2016, art. 4(3b)). An incident with the security of personal data is referred to as a personal data breach. Security is here denoted as an

encompassing term to define any type of incident with personal data. A breach of security leading to "*the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed*" is denominated as a personal data breach (GDPR 2016, art. 4(9)). Required measures to be taken once a personal data breach is detected are further specified in the NIS (chap IV and V) and in the GDPR as a notification requirement.

3.2.2. Processing

As stated earlier, data becomes personal data only when the said data are processed with the intention or ability to identify a natural person directly or indirectly. This definition suggests that data, when viewed in its natural unstructured form by a human being, may not be automatically considered personal data. Nor will such data therefore fall under the protection of the Regulation. Processing steps are defined as the means of:

> any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (GDPR 2016, art. 4(1))

Processing of such personal data that is considered belonging to a special category by parties such as employers, insurance and banking companies, should not be performed (GDPR 2016, recital 42b). To limit the effect of technological progress and the risk of circumvention, the Regulation should be considered technology agnostic. This also suggests that simply adding a manual step in the process does not limit the data subject's protection for personal data. Provided that data are collected for storing purposes with the ability to henceforth indirectly identify the individual, it is considered to fall under the Regulation. In recital 13 (GDPR 2016), an exception to this rule is specified in the case a file or set of files are processed where data are not in a structured format in regards to a "specific criteria". Such a file can e.g. be assumed to be any web page or document that consists of unstructured text. This exception can be considered to permit the search engines to index all publicly available web pages as long as no storage of ordered data that fall under the definition of personal data occurs. There are also considerations that limit the exception. As was highlighted by the Court of Justice of the European Union (CJEU) in the case Google vs AEDP and Costeja (Case C-131/12)[24], an individual's fundamental rights may be considered over the general public's interests (see section 4.3 in this thesis for a methodical case analysis). In a case where personal data are

[24]Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. (2014). Court of Justice of the European Union (CJEU), Case C-131/12.

transmitted outside a certain Member State, the term cross-border processing is used to signify either that processing takes place in several Member States or is likely to substantially affect data subjects in several (≥2) Member States.

3.2.3. Actors

Several actors that require definitions exist in the Regulation. The term actor is here used for the purpose of identifying an entity involved in a specified role in the process. The data subject has already been defined indirectly as the natural person who is identified by the personal data in question. The controller is someone who determines the purpose and means of processing of personal data. The controller is also the original collector of data subject consent. A controller is defined in the regulation as following: "*…natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data…*" (GDPR 2016, art 4(5)). The definition of the controller is similar to the definition in the Directive, although in the revision process the word "conditions" has been considered. The original proposal stated "*purposes, conditions and means of the processing*". That "*conditions*" was deleted from the proposal can be related to the complexities of defining all conditions in a cloud environment that is controlled by some third party and sold as a service that employs virtualised hardware. A processor is defined as follows: "*…[n]atural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.*" (GDPR 2016, art 4(6)) This definition is equivalent to the definition in the Directive. In case a controller uses an external processor, it should be the controller's responsibility to verify that the processor handles the personal data as predefined through the purposes and means of processing. The processor cannot redefine the purposes or means of processing. This is often accomplished through a service level agreement that also ought to stipulate what can be done in regards to personal data. Once personal data has been processed and the result is disclosed to some party, this party is referred to as recipient. The recipient is not necessarily a third party, but can also be the data subject, the controller, or the processor. The third party is then defined by the "*persons who, under the direct authority of the controller or the processor, are authorized to process the data*" (GDPR 2016, art 4(7a)).

Children receive a stronger protection than other data subjects in the Regulation. The controller has the responsibility to determine if a child is the intended data subject. In such a case, the processing is only lawful with the consent of the parent. A data subject is determined to be a child below the age of 16, or a Member State defined age no younger than 13 (GDPR 2016, Art. 8). The use of personal data of children for the purposes of marketing, creating personality or user profiles, and the collection of child data when using services offered directly to a child are

discouraged, but lawful if consent is obtained from a parent (GDPR 2016, recital 29).

3.2.4. Lawfulness of processing

The regulation puts forward several principles to determine the lawfulness of processing for private enterprises. The controller should process personal data in a transparent and fair manner in relation to the data subject (GDPR 2016, art. 5 (1)). To achieve lawfulness in processing (GDPR 2016, art. 6(1)), we can categorise the options as fulfilling one of the following requirements:

Through consent by the data subject,
for the performance of or in anticipation of a contract between the data subject and another party,
through legitimate interests of a controller or other party that may provide a legal basis,
in the public interest (see section 4.3.).

In addition to these categories, personal data can be processed if authorised by public authorities for reasons of safeguarding a democratic society. Lawfulness through the consent of a data subject is the recommended principle to follow and the only principle that receives an explicit definition in the regulation. Consent means "*any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.*" (GDPR 2016, art. 4(8)). The consent agreement can be achieved in any type of statement; however, the controller may need to produce evidence of such an agreement at a later stage. There is a requirement that the data subject needs to actively accept such an agreement and therefore silence or pre-ticked boxes do not constitute consent (GDPR 2016, recital 25). Asking for the consent should not be unnecessarily disruptive to the use of the service, as to discourage users from declining consent. The user should also be able to refuse or withdraw consent at any time without detriment (GDPR 2016, recital 25 & 32). For consent to be considered freely given, it must allow separate consent to be given to different data processing operations (GDPR 2016, recital 34). For processing of special categories of personal data, the data subject should in general give explicit consent (GDPR 2016, Art. 9 (2) point a).

Processing of personal data can also be based on the performance of a contract or in anticipation of the data subject entering into a contract (GDPR 2016, Art. 6 (1) point b). A contract is not defined in the GDPR, but can in the digital environment be assumed to be linked to the provisioning of a service to a user. We can assume that the processing on many platforms are done using a combination of contract

and consent (cf. Facebook Terms of Service[25]), where the contract establishes lawfulness and consent is sought as a secondary assurance. In this case we may assume that the consent agreement in practice is obsolete and that contractual autonomy is considered to fulfil the right to self-determined data processing (Moser 2016). The contract is a legally binding and enforceable agreement with specific terms between the data subject and other entities, in which there is a promise to do something in return for a valuable benefit known as consideration (Contract [Def. 1]). In the digital space a contract is established based on the initiative of the controller, if there is no other legal requirement. For digital services, this means a contract is often of a unilateral nature. A unilateral contract is a promise by the offeror to pay or give other consideration in return for actual performance by the offeree (Contract [Def. 1]). However, a contract does not necessarily require that a monetary transaction is performed between the data subject and the controller for the use of a service. A contract defines the following factual elements:

> a) an offer; b) an acceptance of that offer which results in a meeting of the minds; c) a promise to perform; d) a valuable consideration (which can be a promise or payment in some form); e) a time or event when performance must be made (meet commitments); f) terms and conditions for performance, including fulfilling promises; g) performance. (Contract [Def. 1])

The e-Privacy Directive (2002/58/EC, amended by Directive 2009/136/EC), defines contracts for public communications services (art. 20). The directive requires, inter alia, that a contract should state that:

> details of prices and tariffs, the means by which up-to-date information on all applicable tariffs and maintenance charges may be obtained, payment methods offered and any differences in costs due to payment method;

When the consumer subscribes to services providing connection to public communications services, consumers have the right to a contract with the company undertaking providing such services. As this is a Directive, and each Member State implements separate legislation, it has led to some confusion regarding its scope. The e-Privacy Directive applies to companies offering electronic communications services, e.g. telecommunication companies, but in most cases exclude information society services (Aldhouse and Upton 2015). However, if a company is defined to belong to the category of providing public Internet communications services, then the contract should clearly state any prices and tariffs, including payment methods. Should payment be performed through the collection and processing of user data, it stands to reason that a specific and detailed charge and/or value, is determined for any services rendered. In extension, this ought to be considered for any digital service offerings through terms of service specification. This would be a key facilitator for consumer choice and effective competition in a competitive market

[25] Facebook Terms of Service as of 30.1.2015, Accessed 22.09.2017, https://www.facebook.com/terms.

for digital services. Being able to withdraw from a contract for lawful processing, based on informed consumer choice, such as understanding the true cost of using said service, should form the basis for giving consent.

Several types of legitimate interests to process personal data not explicitly defined in the GDPR art. 4 exist. A public authority can be considered to act with legitimate interests when enforcing the rule of law. Scientific or historical research, as well as archiving, can also be seen as legitimate reasons (GDPR 2016, recital 125). Particularly social and health sciences receive a broad mention where combining registers and performing longitudinal research can reveal important results that justify the processing of sensitive data (GDPR 2016, recital 125aa). A company can also have legitimate reasons to process personal data when it comes to protecting its vital interests, which is necessary for the establishment, exercise, or defence of legal claims. Such examples can be utilisation of active network security methods or securing intellectual property rights. The former may include anonymised traffic meta-data. The latter example can arguably allow the intellectual property rights holder to collect network IP-addresses of users that are sharing material thought by the said holder to infringe on its rights.

3.2.5. Automated Decision-Making and Profiling

Whereas processing refers to the complete process of handling personal data (any operation), automated and specific processing regarding the individual over time is referred to as profiling. As such, profiling of data subjects is regulated further than processing. The regulation defines profiling as meaning "*any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person,*". Examples of profiling provided in the law text are *"in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*" (GDPR 2016, Art. 4 (3aa)). The law text separates the terms profiling and a broader automated decision-making action. The main difference can be seen as the term profiling is mostly used when processing is done for a predictive or prescriptive purpose, e.g. direct marketing where continuous tracking of the individual is the basis of the analytical decision-making for future needs. Tracking of data subjects can for example be done by recording the physical location of the subject, used IP-addresses, storing cookies in the browser environment, device fingerprinting, or recording other behaviour or attitude-related data. These methods are often used in combination to improve the ability to follow the subject more closely. According to art. 15 in the Data Protection Directive, every person has the right not to be subjected to automated processing of personal data. An almost identical rule has been taken into the Regulation (GDPR 2016, art. 20). The right not to be subjected to automated processing covers only measures that produce legal effects concerning the person, or which significantly

affect the person. If the automated profiling produces legal effects concerning the data subject or significantly affects the data subject, it requires consent from the data subject concerned (Bygrave 2001). In addition to consent, there is a requirement for suitable technical safeguards to prevent any potential abuse. The Commission is empowered to further specify the criteria and conditions for suitable safeguards.

3.3. Summary

In relevance to RQ1, chapter 3 outlines the applicability of the GDPR and the processing of personal data. Processing refers to the complete process of handling personal data, from the collection to any decision-making. Profiling refers to a specific part of the processing procedure, namely the analysis or prediction of aspects concerning a natural person's performance based on personal data.

GDPR recommends as a minimum precaution that personal data be pseudonymised before being stored, particularly if data are stored long-term. Where possible, the controller should try to anonymise data belonging to a special category. This implies for example that such traffic meta-data that is not needed for service personalisation, but where data can be used at a later stage for some other purpose, should be anonymised (cf. RQ2). The method difference refers to anonymisation as the aim of irreversibly preventing the identification and pseudonymisation as the replacement of any identifying characteristics of data with a pseudonym (Data Protection Commissioner 2017). Provided the source data are deleted, irreversibly anonymised data are then no longer considered personal data. Several researchers have questioned the effectiveness of these privacy-by-design methods and have shown that de-anonymisation attacks can re-identify the data subject (e.g. see Wondracek et al. 2010; Narayanan et al. 2012; Ma et al. 2013).

The classification separation between both normal and special categories of personal data may at times result in difficult design choices. For example, an image is considered under special categories when used for identification and/or authorisation, while in documenting a care story the same image may be considered personal data. Assuming the data subject has manifestly made the image public outside the immediate family, the system may in some cases be allowed to process the image at its own discretion (Pulkkis et al. 2018).

Anonymised genetic data offers another challenge, because if the physical link to the data subject is removed, then the genetic data should be relatively free to process. Still, de-anonymisation can perhaps not be performed by using a secondary register, but as long as the individual is alive, a secondary register exists. If the individual at a later stage permits a secondary genome sequencing, a link to any processing of the first sequencing, may be performed. Additionally as the genome is heritable, any offspring may also be identified at a later stage. Consequently, it stands to reason that genetic data should always be treated as personal data. A partially similar argument can be done in regards to biometric data.

Determining lawfulness of processing and to subject a natural person to automated decision-making through profiling, is regulated in the GDPR. Management support systems (see section 2.3) that are using personal data will consequently be affected (cf. RQ1). Decision support systems that allow a human operator to interact with decision algorithms may fulfil the requirement that a data subject has the right not to be subjected to a fully automated process that uses personal data. The use of expert systems (e.g. automated intelligent agents) which produce legal effects that concern the natural person or significantly affects the person is limited by the consent of the data subject. The data subject shall at any time be able to understand the use of automated decision-making and be able to revoke the consent for the use of such automated decision-making.

As the centralised governance model is the common manifestation of the platform today, this is discussed in section 2.7. In Enkvist et al. (2017) we discuss the application of a decentralised platform, which is governed through the decentralised execution of smart contracts on a blockchain (cf. RQ3). Although someone has to construct these smart contracts, their execution is fully autonomous. The question then becomes if the data subject wants to exercise his right not to be subjected to autonomous decision-making, who should become an operator, or whether the decentralised blockchain platform is unlawful, provided that it is handling personal data. Autonomous software and platforms designed on the principals of "code is law" (Lessig 2000) can thus be seen as problematic from the consent seeking GDPR, thus we can assume that the lawfulness can best be achieved through contract. The Ethereum blockchain is often considered an example of the "code is law" principals (Filippi and Hassan 2016). In a decentralised system, there may neither be a central power with the ability to insert individual transactions as this requires consensus nor a single point or node of failure (Raval 2016). In the case of cryptocurrencies such as Bitcoin, the GDPR is only applicable if the natural person can be identified. The Bitcoin wallet address is public and any transfers to or from the wallet can be tracked. For example, once a traditional bank account is used in transferring funds into the wallet, the physical link can be determined by the facilitator of said transfer. Still, this information is not necessarily public, nor is the data linking the wallet address to a bank account published on the blockchain. Thus, we can assume that the Bitcoin blockchain itself does not fall under the GDPR. The omission of protection for virtual identities is further discussed in sub-section 4.2.5. However more advanced use cases and developments of blockchain-enabled platforms presented by Honkanen (2017), show that personal data may in the future be stored on the blockchain. This development will be interesting from the perspective of decentralised business models and their compliance to the GDPR.

We can only see a short distance ahead, but we can see plenty there that needs to be done.

— Alan Turing

4. Regulatory Design Implications

The Regulator has emphasised that the Data Protection Regulation should be technology agnostic, thereby hoping that technological progress should not directly render the law invalid. From a technological perspective, obstructive legislation that hinders the development of new technology should be avoided. Instead, we should always strive for a law text that allows for diversity in technology and digital services.

The following chapter examines the legislation from the design perspective of information systems. Interpreting the challenges the legislation transposes on information systems and determining the limitations in scope of the legislation is of interest to both the information systems researcher and system creator alike. The intention is to deepen and thereby connect the earlier discussion in chapter 3 with technological aspects often encountered in the design of information systems and in particular intelligent services. I intend to achieve this through detailed examples (use cases) of chosen areas and link up with core themes in the Regulation, regarding aspects of automated processing.

4.1. Personal Data

Over the years the definition of personal data has raised some important questions concerning what is covered by the definition. Some guidance in connection to this was already given in Recital 26 of the Data Protection Directive. A category of data that has been extensively discussed with regard to whether it is covered by the definition of personal data or not is IP addresses, especially dynamic IP addresses. The Article 29 Working Party[26] has been arguing that not only static IP addresses should be considered personal data, but also dynamic IP addresses should fall under the definition (Article 29 Working Party 2007). This point of view has also been taken in the Regulation. The Regulation has much of the same wording as the Data Protection Directive, but in the Regulation online identifiers have been added to the text (GDPR 2016, Art. 4(1)). The original proposal considered that online identifiers as such are not necessarily to be considered as personal data in all circumstances (draft Regulation, Recital 24). In the GDPR (2016) this ambiguity has been removed.

An important question relating to the definition of personal data is how the word identifiable should be interpreted. To be identifiable it has to be possible to identify a person, which suggests that the meaning of the word includes some grade of probability (Vaidya et al. 2006). The Data Protection Directive and the Regulation does not implicitly give any guidelines regarding how big the possibility has to be. It has been considered that a mere hypothetical possibility to single out the

[26] Article 29 Working Party has an advisory status to the EU Commission, acts independently, and is mostly composed of Member State data protection supervisory authorities.

individual does not fulfil the requirements, though (Article 29 Working Party 2007). Recital 23 of the original Regulation stated that account should be taken of all the means reasonably likely to be used, either by the controller or by any other person, to identify the individual. This was criticised for being unclear (Westerlund and Enkvist 2013). What is reasonably likely to be used can differ from situation to situation. A mere hypothetical possibility to identify a person is not enough. The deciding factor is what kind of means will likely be used to identify persons. One of the most important factors deciding what the means are for identifying a person will be based on a cost-benefit analysis by the processor (Article 29 Working Party 2007). Technical development can also change the situation regarding what is reasonably likely to be used. New techniques and technology may make it much easier to identify persons (Costa and Poullet 2012). Therefore, the definition of a data subject is not static; it will change over time alongside the technical development. In the GDPR (2016), the term 'reasonably likely to be used' has been removed. This suggests that the burden of proof is still with the controller, but now the controller is e.g. no longer evaluated against its peers or technology in general, but rather in its own capacity.

Both the Data Protection Directive and the Regulation make a distinction between common personal data and special categories (sensitive) personal data. Processing of sensitive personal data, e.g., race, ethnic origin, religion, health and sex life, is in principle prohibited and is only allowed under certain exceptions. However, the Regulation does not give an answer to which category such sensitive data that have been derived through processing of common personal data belongs. Using combinations of data-processing techniques makes it possible to create such information that can be regarded as sensitive. This information does not need to be labelled as e.g. race and religion, but rather as a cluster of people that belong to unspecified groups. It may be possible for a processor to correlate this synthesised information with data belonging to special categories, if this data can be accessed, but in most cases e.g. visiting a place of worship at a particular location or weekday is already a strong enough indicator of religion and in some cases race. With regard to a strong protection of data subjects, such derived information should be considered to be sensitive, and therefore allowed only under certain exceptions (De Hert and Papakonstantinou 2012). Hildebrandt (2009) goes further, arguing that no differentiation between data and sensitive data should be made, because highly sensitive information can be inferred from seemingly trivial and anonymous data. This is also very much in line with the view of this thesis. Insights gained during profiling should always be considered as potentially sensitive (cf. RQ1). Synthesised data and eventual decisions made based on these insights should therefore require an explicit consent from the data subject. In the construction of information systems, this should thus influence design choices, as automated decisions concerning a data subject must be transparent. When employing machine learning

algorithms that are by nature non-deterministic, particularly such algorithms that are not provided a goal (e.g. unsupervised learners), there is an imminent processing risk that needs to be communicated.

4.2. Profiling and Tracking data subjects

Profiling and tracking are among the most important tools a company or professional (e.g. a marketer) can employ to understand and anticipate the customer's needs. At the same time, these tools can be used to exploit a data subject against his will. For example, with the help of profiling marketing professionals can target tailored and behaviour-based advertising to individual recipients, i.e. personalised marketing. The transition to the digital society has made us leave an increasing number of electronic footprints behind us. With the help of these footprints, detailed profiles of individuals can be drawn up. Earlier, both the technical infrastructure and the high cost were a barrier for the development of detailed profiles of data subjects. The transition from centralised IT-architectures to scalable and distributed solutions, such as the MapReduce-model by Google, has removed the obstacles concerning infrastructure. As discussed in section 2.5, scalable architectures in principle make it possible to scale out the calculations horizontally, merely by adding more hardware. In addition, the high cost of preparing detailed profiles has been minimised due to the development of cloud computing and the possibility to rent virtual hardware. Recently, the development of so called 'Analytics as a Service' has lowered the cost barrier further, as the employment of advanced models can now be performed without first having to develop costly software in-house.

In the subsequent sub-sections, the discussion focuses on some of the technological implications of the GDPR (cf. RQ1). The intention is to develop an interpretation of the GDPR in order to understand the limitations and ambiguities in implementing such processing of personal data that leads to profiling and automated processing. The analysis of the law text is not intended as a critical or negative examination, but rather as a way to determine how analytics developers should understand the text.

4.2.1. Consent

The definition of consent in the Data Protection Directive (Art. 2(h)) has led to various interpretations in different EU Member States. Some Member States, e.g. Finland, accepted that passive behaviour fulfils the definition of consent in the Data Protection Directive. According to the Article 29 Working Party, passive behaviour should not be seen to be in accordance with the word "indication" (Article 29 Working Party 2011). For processing of sensitive personal data, the Data Protection Directive (art. 8) requires that the consent is explicit.

As highlighted in sub-section 3.2.4, several provisions for achieving lawful processing exist. The definition of consent in the Regulation demands that consent must be explicit to the purpose of processing. Consent for processing common personal data and sensitive data therefore have the same requirement of consent. In Recital 25 of the Regulation it is expressly stated that silence or inactivity do not constitute consent. The requirement of explicit consent does not mean that the consent has to be given in written form (Lynge 1995). It is possible to give explicit consent e.g. by ticking a box on a website. A significant change was inserted in the original Regulation (art. 7) that consent shall not provide a legal basis for the processing when there is a significant imbalance between the data subject and the controller (cf. RQ3). Bräutigam (2012) considered that platform companies like Facebook would find this particularly problematic to achieve. In the second public draft the text had changed, and in the third draft of the proposal this article had been deleted. However, in GDPR (2016) Article 7 has been re-inserted; when assessing whether consent is freely given, account shall be taken of whether the provisioning of a service is made conditional on the consent for the processing of data that are not necessary for said service. Recital 34, was again amended to include the following interpretation:

> In order to safeguard that consent has been freely-given, consent should not provide a valid legal ground for the processing of personal data in a specific case, where there is a clear imbalance between the data subject and the controller (GDPR 2016).

That consent shall be freely given means that there shall be no constraint or pressure on the person giving his or her consent (Solove 2013; Cleff 2007). There has to be a real possibility to give consent or not for the data subject. The requirement of freely given consent shall not be interpreted to prevent for example websites from using some kind of consequence(s) for a person who does not give consent. For example, charging a small fee for using the service when no consent has been given, while persons who have given consent can use the service for free, should be interpreted to fulfil the requirement of freely given. If a refusal of consent prevents a person from using the web service, it can be argued that the requirement of freely given consent is no longer fulfilled. This particularly concerns incumbent platform companies like Facebook and Google, who can be considered to be in a dominant market position in their respective domains. Another particular category of companies is those that provision services to children exclusively or unexclusively.

As mentioned earlier, both the Data Protection Directive and the Regulation make a distinction between common personal data and special categories personal data. This raises the question whether one given consent can be interpreted to cover both categories of personal data (cf. RQ1). A consent given for processing sensitive personal data may in some cases be considered to cover also processing of common

personal data. For sensitive personal data the consent must be made specific to the processing task and therefore if that task also includes processing of common personal data it should be seen as valid. Consent given for processing common personal data should not be considered to cover sensitive data. If the controller will/can synthesise sensitive personal data from the common personal data, then the data subject ought to give an explicit consent to this as well.

The data subject has the right to withdraw his consent at any time (GDPR 2016, art. 7). To be effective, this rule should require controllers and/or processors to uphold a web page or similar service, in order to inform the data subject what he or she has given consent to. This becomes even more important for platform companies, which uphold a diverse set of services (RQ3). Otherwise the data subject will have great difficulties withdrawing each consent given to every single party and altering this consent at a later stage. This should not mean that a service provider is required to employ an identification and authorisation service for users, but it can also be based on other tracking mechanisms utilised by the controller. This will thereby let the data subject review what is currently known of him, what he has consented to, and the possibility to remove specific consents. Hence, if the controller has stored a cookie (or uses any other mode of tracking that involves storing data) on the data subject's device and this identifier is linked to a consent agreement in the controller's service, then the data subject must be given a way to review or amend this information.

4.2.2. Profiling

By employing profiling, the advertiser for example is capable of sending the recipient tailored advertisements. As earlier stated, according to the Regulation (GDPR 2016, art. 20) a person has the right not to be subjected to a decision (e.g. based on profiling) that is based solely on the automated processing of data, provided it is not needed for fulfilling a contract. The Right is linked to the outcome of such processing; because it only applies if legal effects are produced concerning the person or otherwise significantly affects the person. What defines "to be affected" is not explicitly determined. For instance, if the automated profiling produces a suggestion to view certain material on a web site, will the user then always be affected (cf. RQ1)? The assumption should be that any measure taken to influence the subject in some way, based on automated processing, requires consent from the data subject concerned.

According to art. 17 in the Regulation (GDPR 2016), the data subject has the right to require the controller to erase all personal data on himself. Even if it is not stated clearly in the Regulation, this could be interpreted in a way that the data subject has the right to require erasure of profiles built through profiling (RQ1). It is important for data subjects to be aware of the results of profiling, in other words to be able to object to profiles they do not find appropriate. Art. 11 in the Regulation

also emphasises the importance of transparent information. The information relating to the processing of personal data must be in an intelligible form and consist of clear and plain language.

4.2.3. Defining the processor of client-side profiling

The revision of the HTML standard enable developers to create web applications that resemble native applications both in responsiveness and persistence capabilities. The HTML5 (2014) and forthcoming HTML5.1 recommendations bring with them a fully-fledged local storage capability for a client application running in the browser. The recommendations add three new technologies (Application Programming Interfaces, API) implementing offline support for web applications[27], namely Service Workers (Russel et al. 2016), Web Storage (Hickson 2013) and Indexed Database (Mehta et al. 2012). The Service Worker is a generic handler for event-driven background processing (incl. offline) in the client application that responds to events dispatched from documents and other data sources. A system for managing installation, versions, and upgrades is provided. Web storage will give the developer access to a key/value-like data structure that can be set to exist for only the session or to be permanent. The web storage technology resembles and to some degree substitutes, the use of cookies, but it can be considered more robust. The Indexed Database API allows for more complex and indexed object data structures to store large amounts of data in so-called object stores. The browser will limit access from client applications to data originating from within the same domain (sandboxing). The client-side sandboxing neither limits data transfers on the server-side nor client-to-client, provided this transfer mechanism is built into the service. It should be recognised that the utilisation of these storage technologies should require consent or a contractual agreement from the user, as they currently can be considered bound by the e-Privacy Directive art 5(3) when used for tracking purposes. In particular, this should apply to services that allow several users of a device access to the same account and the data connected to the account. A platform or service should always strive to ensure that data are protected from other users of the same device, before initiating tracking and/or profiling (cf. RQ1 & RQ3).

This new technology unlocks the possibility of building rather advanced web application clients. An example is email clients in the web browser that store all email data locally; the client can also store many other types of user statistics, e.g. search keywords, likes, and any other platform-related feature. Assuming that the service provider implements a direct marketing profiling system directly into the web client. The system would allow the provider to target advertisements to the user by using personal data, sensitive or not. Accessing only locally stored data and processing the data only locally and then simply fetching a certain class of

[27] The browser creator can choose to implement support for some or all APIs.

advertisements, opens the definitions of controller and processor in the Data Protection Regulation to interpretation.

A provider who distributes an application that uses client-side profiling can be argued to fall within the definition of a controller (cf. RQ1 & RQ3). The service provider determines the purposes, conditions, and means of personal data when the application is being distributed. However, the situation is not that clear after the system is stored locally. Once the system is stored locally and the processing of data proceeds only locally, without the insight of the controller, there could be ambiguity regarding whether the controller still determines the purposes, conditions and means of the processing. However, it would not be reasonable to interpret the Regulation in such a way that the controller would be free from obligations once the system is stored locally.

Processing has been given a very broad definition in the Regulation. Client-side profiling will without doubt fall inside the definition of processing. In client-side profiling, the processor would be the data subject himself. It is not clear whether the definition of processor in the Regulation, also covers the data subject. There are, however, no expressed restrictions in the definition, whereby even the data subject should be interpreted to fall within the definition of processor. On the other hand, the aim of the regulation is to protect data subjects, and a contract between the controller and processor will always be required (GDPR 2016, art. 26(3)). Therefore, to interpret data subjects as processors would, to some degree, contradict the general aim of the Regulation. Consequently, if a processor cannot be determined, it is unclear whether any party holds the obligations of the processor. The example shows there is still a need for a clearer definition of the term processor. In this case, if the processor's obligations are not with the controller, it suggests that any sensitive information can be used for profiling purposes, provided that the controller does not hold the means for identifying the natural person. Therefore, client-side profiling as a technological solution for improving data security, should be strived for (cf. RQ2).

Although client-side profiling is here described by implementing it in the web application, it can also be implemented in the browser directly or in a browser plugin, as well as in any device application. The reason we chose to describe client-side profiling as a web application is due to the simplicity, it can be done by anyone providing a web presence, signifying that a user only has to visit the web site, while the other examples require the user to download and install software first. In the example, when the user visits and loads the web page for the first time, the application logic and required data structure schema is transferred at the same time. Afterwards, each time the user communicates with the web service, all processing and profiling can occur in the client. Real-time browser-to-browser communication capabilities with a new communication protocol called WebRTC have been proposed (Bergkvist et al. 2017). This potentially enables synchronising personal

data between the web clients of the data subjects without a central storage node provided by the service provider. Considering then that the service provider, i.e. controller, no longer is performing the processing (incl. storing data), nor is a third party involved, we can argue that the controller cannot determine the physical identity of the individual. As stated earlier, being able to identify the physical identity of the individual directly or indirectly, is a prerequisite for the Regulation to be applicable.

4.2.4. Tracking of users

Tracking users on the Internet can be performed in many ways. The topic of using different types of tracking mechanisms have been extensively debated in both legal and technical literature (e.g. see Enkvist-Gauffin (2006)). The practise of tracking users has also received a lot of attention from EU lawmakers and is regulated in the Directive on privacy and electronic communications (e-Privacy Directive 2002/58/EC; 2009/136). A significant change brought by the e-Privacy Directive was the requirement of prior consent before storing information (tracking mechanisms) on the device of a user (art. 5(3)). Enkvist-Gauffin (2006) considered the prior consent requirement as an opt-in mechanism, were users had to give consent prior to tracking being initiated. The e-Privacy Directive does not however define a tracking mechanism per se, but a broader storage procedure, as it is defined as that "*to store information or to gain access to information stored in the terminal equipment of a subscriber or user*" (recital 66) requires consent. Nowadays, state-of-the-art techniques employ more advanced methods for tracking, as storing cookies on a device is not reliable enough and cookies are easily deleted by the user. Cookies can still be a part of tracking, but as the modern user is no longer confined to a certain device, service providers want to be able to identify the individual among the myriad of devices. This can be done by using a combination of techniques, but at its centre is often a global social media platform that requires the user to log in to its service (cf. RQ3). When the user identifies himself to the social media company, they become able to track the user, even if the user exits from the said service, when browsing other sites that use the tracking software developed by the aforementioned. Typically, tracking is done through the implementation of social network widgets. This way user activity can be traced in terms of the user's browsing behaviour.

The way users were traditionally tracked was by recording the IP-address, but as the use of mobile broad band increases, using IP-addresses has become an unreliable method. Instead, software developers have created a browser (device) fingerprint from various other identifiers describing the machine (e.g. installed browser fonts or plugins). Although the browser fingerprint is not considered stable in the sense of giving a unique identifier in all cases, it is still considered quite reliable when combined with other techniques such as location segmenting (e.g. based on client

time-zone or IP owner) (Eckersley 2010). As the browser environment changes, the user installs new fonts or plugins, the browser fingerprint is no longer the same. Then other methods can be used in combination to detect that it is still a known user to the service provider. Regarding smartphones, when a user installs an app, then each sub-sequent usage session of the app can be used to uniquely identify the same device. The app may also access a unique identifier for the device, which can be used server-side to link a user's behaviour between two or more apps using the same technology.

As stated earlier, if a company uses IP addresses to track users it is usually considered to be an identifier that can be used to identify a natural person, and is therefore protected by the Regulation. The same applies for cookies or other information being stored on the device for achieving a tracking ability of an identifiable natural person. However, direct marketing or price quoting on the Internet often have little interest in identifying the natural person, the interesting part is the online behaviour of the data subject. Considering the volume of data amassed on data subjects, the velocity of staying updated and the data variety describing users, as big data often is defined (Laney 2001), it is no surprise academics consider big data challenging from both a privacy and an integrity point of view (Krasnova & Kift 2012; Kaisler et al. 2013). The definition of tracking methods is broadly defined in the e-Privacy Directive, as a tracking ability. So the main focus is on whether the situation with tracking fulfils the definition of data subject. As mentioned earlier, the definition of data subject is an identified natural person, or a natural person who reasonably can be identified. In the definition of data subject, some particular factors which can enable such identification are also pointed out. The factors mentioned in the definition are identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. This means that different types of tracking techniques must be considered to fall within the scope of the Regulation, including the browser fingerprinting.

4.2.5. Protecting the innocence of children when using information services

An additional concern regarding tracking is how the service provider can detect that children use a certain device. In families, it is often common that everybody in the household uses the same user account to browse the web. When it comes to tablet operating systems, they do not necessarily offer an obvious or easy way for families to separate the usage patterns of adults and children. Children deserve a specific protection of their personal data. This is emphasised in recital 29 to the Regulation. Children need specific protection because they are less aware of risks and consequences in relation to the processing of personal data. According to Art. 8 (1)

(GDPR 2016), the processing of personal data of a child is lawful only if consent is given or authorised by the child's parent. The controller must make reasonable efforts to obtain verifiable consent. An example of such a process is that the child chooses to install an app that will process personal data on the phone, but before being able to complete the process a parent must first consent to the processing. This requires the parent(s) to link their phone account to the child's, before installing the app. There will be significant problems for tracking services to detect whether the user is a child or an adult when it comes to tablet operating systems. The example provided above will also require the parent to be a smartphone user or at least digitally inclined as to solve it some other way. Provided it is extremely difficult for the service provider to detect whether the user is a child or an adult, will it mean that the provider is allowed to assume the user is an adult? Because children are using different kinds of devices with an Internet connection more and more, it would not be a reasonable solution to allow such a presumption. On the other hand, if a child uses a browser to read a digital newspaper, how should the provider of said service determine that the consent to track could not be given by the visitor himself? Today, there is no standardised technology to indicate that the browser user is a child, hence, the situation still needs further clarifications from the Commission. A similar technique as 'do not track' that is implemented in most browsers could be used for indicating that a child is the user of this device. In the browser this is implemented as an HTTP header that is sent to the service provider with the request for a web page.

We should point out that 'do not track' messages are today only respected at the discretion of the service provider. Should the Commission lay out guidelines for requiring service providers to detect user preferences in a generalised way, then the technical implementation for web traffic or rather HTTP/HTTPS requests, is a proven solution. The solution applies to other applications as well, provided they communicate through HTTP/HTTPS requests. Other HTTP headers can also be implemented, e.g. 'do-not-profile' or 'child-using-device' (cf. RQ1).

4.2.6. Virtual identity in an online forum

The recommended approach is that a service provider asks for consent in order to profile users if the information contains direct or indirect references to the natural person. Personalised online direct marketing often works by offering advertisement on the basis of such user profiles. However, in the following example, we consider an online forum requesting users to login to be able to use the service, but asks for or stores none of the information referring to a natural person. While the user uses the service, e.g. browsing other virtual users and befriending them, liking stories or items, or entering search terms or posting messages; using this type of data much information regarding the user is revealed, i.e. data subject (Korolova 2010). When considering the notion of protecting the data subject, it becomes difficult to show

how any of the collected data as such is linked to physical identifiers, and thereby linking the digital profile of the user to a natural person. Regardless of this missing link, the service provider can likely tailor any direct marketing messages and/or pricing information to the data subject almost as easily as if the provider also stored or processed any direct or indirect references to the natural person.

The service provider can, with some probability, deduce new information about the data subject by analysing data as a complete set. For example, an entered search term indicates something that is currently of interest to the subject. A forum posting can be analysed using text analytics to reveal the topic of the posting or the opinion in the posting. Social network analysis can reveal links between various network nodes, be it users or other objects. By using modern analytical techniques in combination, it is possible for a service provider to profile each user in near real-time, for instance, to find out the best direct marketing advertisement to show, without linking the virtual identity to the natural person.

The examples demonstrate how it is possible for a service provider to profile users without the possibility to identify the physical identity of the user (cf. RQ1). This situation will therefore fall outside the scope of the Regulation. The Regulation will apply only to information concerning an identified or identifiable person. Whether a person is identifiable or not depends on the means used in the identifying process. If a service provider cannot identify the physical identity of the user, directly or indirectly, then the Regulation will not be applicable (recital 23).

4.3. Public Interest

One actor (cf. sub-section 3.2.3 and 3.2.4) that is not directly defined in the regulation, but often referred to, is the public interest. Processing based on public interest shall only be used if other means of achieving lawfulness have been exhausted. As showed below, this method is not as straightforward as the other means, as guidance is rather limited and spread out in the Regulation it merits further inspection. Public interest is a multifaceted term that we will attempt to delineate in the following and highlight its connection to intelligent services (cf. RQ1). The section also provides a technical interpretation of the Court of Justice of the European Union Case (C-131/12) that is considered to establish a “Right to be forgotten”.

The data protection legislation sometimes considers the public interest over the data subject’s privacy right, hence the right to the protection of personal data is not an absolute right (GDPR 2016, recital (3a)). Personal data may be lawfully processed if it "*is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*" (GDPR 2016, Art 6 1(e)). That an official authority may process personal data in performing its duties is relatively clear and the cases presented later show this as well. An example is the tax

authorities that may process sensitive information to, inter alia, determine the taxable income. However, there might be circumstances when some other legal person than an official authority can process personal data under the lawfulness criteria of public interest.

We here continue with the assumption that public interest refers to a potential population of undetermined size in a Member State, which does not necessarily include everybody. The CJEU referred to this grouping in its ruling in the case Google v AEPD and Costeja (Case C-131/12). The case pertains to an official notice given in a newspaper of a conviction against Mr Costeja and whether Google is permitted to continue displaying a link to this notice among the search results for the name of Mr Costeja. The opinion of Advocate General Jääskinen (Opinion. C-131/12, 2013) in the given case, was that "*processing of personal data, covers all information relating to an individual, irrespective of whether he acts in a purely private sphere or as an economic operator or, for example, as a politician*" (Opinion C-131/12, Sec C, §118). He continued by defining a search engine operator as a private subject, and on the question if interference, i.e. processing of personal data without consent, can be tolerated, Jääskinen argued:

> it is necessary to ponder whether interpretation of Articles 12(b) and 14(a) of the Directive in light of the Charter, and more particularly of Article 7 thereof, could lead to the recognition of a 'right to be forgotten [over the public interest.] (Opinion C-131/12, Sec E, §126)

The Advocate General considered the right to search information published on the internet, by means of search engines, to be one of the most important ways to exercise the fundamental right to receive information concerning the data subject from public sources (Opinion C-131/12, Sec E, §130 & §131). In the concluding remarks Jääskinen finds that "*An internet search engine service provider lawfully exercises both his freedom to conduct business and freedom of expression when he makes available internet information*" (§132). He continues with:

> reinforcing the data subjects' legal position under the Directive, and imbuing it with a right to be forgotten […] would entail sacrificing pivotal rights such as freedom of expression and information. I would also discourage the Court from concluding that these conflicting interests could satisfactorily be balanced in individual cases on a case-by-case basis, with the judgment to be left to the internet search engine service provider. (Opinion C-131/12, Sec E, §133)

According to the opinion of the Advocate General, the fundamental rights and freedoms cannot in this case be considered to outweigh the public interest in terms of right to receive information nor the commercial rights of the search engine company, as he considers the information at the source to contain an accurate description of historical events.

In the consequent judgment by the CJEU they considered the aspect of privacy as a fundamental right. When:

> [a] search by means of that engine is carried out on the basis of an individual's name [it is likely] to affect significantly the fundamental rights to privacy and to the protection of personal data [...] since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual [thereby establishing a more or less detailed profile of the data subject] (C-131/12, §80).

As stated in sub-section 3.2.1, information on criminal convictions belong to the special category and any structuring with the intention to link the information to a physical individual is generally not permitted. A similar limitation is provided in the Directive (art. 8(5)).

However, the CJEU goes further in its statement by referring to "*the information at issue*", and not necessarily being limited to the information of convictions.

> However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's (C-131/12, §81).

The remedy then ordered by the court is to restrict certain results from being shown, unless a preponderant interest of the public can be determined:

> balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information (C-131/12, §81).
>
> Accordingly, since in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, [...] the data subject may, [...] require those links to be removed from the list of results. (C-131/12, §98)

The decision in certain aspects goes against the opinion of the Advocate General. An interesting aspect of the court's decision is that they actually do not forbid a search engine to provide another source for the information, hence the content does not need to be automatically "tagged" and classified as violating the data subject's rights in question. Also, the verdict states that the links should be removed from the final presentation of the result. From a technical perspective this can be thought of as a filtering approach, and that in this case the search engine is not forbidden to continue processing the pages as long as the links are not included in a search result. From a legal viewpoint, the processing of personal data only occurs when the user enters the name as a search term and the result is delivered to the requester. To understand this argument, we have to consider how a typical search engine operates. Google's particular algorithms for search have not been published, but over the years they have provided some generalised understanding of how it is architecturally constructed. A search engine has a number of different search algorithms, but in the case laid out we can only consider the most basic approach of a search term consisting of a first and last name. Essentially the processing that occurs before the

user enters the search term can be considered irrelevant in this case, because it can most likely be argued that the individual cannot directly or indirectly be identified from this process. First, to find content the search engine uses a crawler agent that retrieves content from a webpage and often stores a copy on the search engine servers. The following step is the indexing of retrieved content that becomes pre-referenced in terms of determining the context relevance for every single page indexed and an indexing of possible search terms that can be construed from the page. Although technically possible, the indexing is not likely to include a specific profile for every single individual identified. The difference here is in whether the data, when pre-compiled by the search engine, has become structured in regard to a specific data subject, which the court did not consider likely. The third step takes place after the user has entered the search term, then search results are ranked and the presentation of the results are sent back to the requester. Here the court finds that the search engine only has to remove the showing of such results that have been contested by a data subject and that in a consequent manual process have been deemed adequately sensitive. The wording of the case, however, does indicate that certain processing by a private (legal) subject is permitted under public interest, provided that intrusive data for a data subject is not shown in a structured form.

The court's decision may be considered controversial, but not particularly unexpected. The original GDPR proposal (COM(2012)11) included an article named *The right to be forgotten and erasure* as an elaboration from the right of erasure provided for in Article 12(b) of the Directive (95/46/EC). In a later revision of the proposal this article has been re-named *The right to erasure* (GDPR 2016, Art. 17). The article makes the definition, which was under consideration before the CJEU (Case C-131/12), somewhat clearer. According to Art 17 (1)c, if the data subject objects on the grounds of Article 19 (1) (Right to object), to processing based on lawfulness of processing for the performance of a task carried out in the public interest (Art. 6 (1)e), then the processor shall no longer process the data unless compelling legitimate grounds can be presented. Generalising the legitimate grounds can be challenging. However, in Article 9 (2)e, processing of special categories is allowed if the processing relates to personal data which are manifestly made public by the data subject. The term manifestly made public has not been defined, but the adverb manifestly can be defined as 'obvious to the eye'. In a Canadian Case (Murphy v. Perger) the Court came to the conclusion that the invasion of privacy to the data subject was minimal for Facebook postings of images, even if they are kept within a private sphere. The Facebook profile in the case included 366 friends and the posts were only viewable by this group. Such a posting was then referred to as being manifestly made public. Here we should stress that the EU courts may have a different definition as to what constitutes manifestly made public, but it can be considered indicative of one-to-many communications.

In recital 36 (GDPR 2016) we find that it shall be up to:

> Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or by private law such as a professional association.

This suggests that processing based on public interest may be interpreted differently in Member State law and that continued fragmentation will exist for processing based on public interest. However, this should not necessarily be considered a politically driven agenda, but may rather stem from a necessity due to other incompatible member state laws. Recital 40 also states that processing of personal data that has been collected for other purposes may be permitted for the performance of tasks carried out in the public interest. This processing may be further determined by Union or Member State law. Further processing for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes are considered compatible and lawful processing operations. Other specified reasons are vital interests of the data subject (or in limited instances another subject) as for example when processing is necessary for humanitarian purposes (GDPR 2016, recital 37) and to safeguard a democratic society (recital 40). Member State law may require controllers to consult with, and obtain prior authorisation from, the national supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest (GDPR 2016, art 34 (7a))

Although the GDPR does not specifically provide guidelines for processing under public interest, certain general guidelines are provided to determine the legal basis for processing of personal data for other purposes than the purposes for which the data have been initially collected. To ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller should consider, inter alia:

> *any link between those purposes and the purposes of the intended further processing,*
> *the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use,*
> *the nature of the personal data,*
> *the consequences of the intended further processing for data subjects,*
> *and the existence of appropriate safeguards in both the original and intended further processing operations.* (GDPR 2016, recital 40)

To define the appropriate safeguards for processing based on public interest, we can consider earlier court proceedings in regards to processing based on official authority. In the Case (24117/08) Bernh Larsen Holding AS and Others v. Norway, the court held that tax authorities are classified as performing a public interest duty that overrides the individual's privacy rights. The court emphasised that the tax

authorities had effective and adequate safeguards in place to prevent potential abuse and that data would be immediately deleted once no longer needed. A task carried out by a vested authority overrides the data subject's privacy right, provided that necessary safeguards exist and that data is deleted in the controller's (or someone who processes the personal data on behalf of the controller) system(s) as soon as it is no longer needed. A third relevant principle that can be considered is the data minimisation principle. In the Case (C-524/06) Heinz Huber v Bundesrepublik Deutschland the court found that German authorities may keep a register of foreigners currently residing in the country, provided that the register only contains information directly required for performing an evaluation of the right to residency. In the event of an official authority outsourcing the processing to a processor, it should not influence this standpoint, provided assurances are given that the security principles defined are followed.

The interpretation of lawfulness for a private legal person to process based on public interest indicates that under certain settings it can be applied to personal data:

where data has been obtained from the data subject, but for another purpose,
where data has not been obtained from the data subject,
where data has been manifestly made public (incl. special category).

Provided that the controller can show that a preponderant interest of the public exists without causing potential harm to the data subject, for example through a data protection impact assessment, the national supervisory authority may grant such processing. In performing a data protection impact assessment the controller evaluates, in particular, the origin, nature, particularity and severity of a risk to the data subject. When data has not been manifestly shared by the data subject himself, then processing can be challenged, as was done in the case before CJEU (C-131/12). It should be pointed out that this interpretation of lawfulness is, to the best of the author's knowledge, not evidenced by EU case law.

4.4. Summary

There are two important concepts in the GDPR (2016 Article 5(1) a), personal data shall be processed fairly and in a transparent manner in relation to the data subject. For the adoption of intelligent services that for example utilise data from IoT-sensors, the GDPR may add additional system challenges compared to today's regulatory environment (cf. RQ1 and RQ2.1). We can draw three main considerations on how to achieve system compliance with the GDPR:

Design requirements
- requiring freely given consent or
- by contract or for the performance of a contract
- data minimisation
- data protection by design and default.

Handling of personal data

- access
- rectification
- portability
- transparency of usage
- erasure.

Limitations on processing

- notification
- restriction
- security. (Pulkkis et al. 2018)

Quality of personal data from IoT-sensors or other data generators must, in light of the GDPR, be accurate and reliable. The data itself must be electronically transferable, though the GDPR does not elaborate on the use of transportation medium. Meta-data describing, e.g. data source, access rights, and justification for lawful processing should be recorded along with the data when it becomes associated with a natural person (cf. RQ2). During feature engineering, such efforts must be made that descriptive statistics do not infringe on the data subject's integrity or introduce new features that can be considered sensitive (cf. RQ1). An example of the creation of new features can be clustering based on location and additional externally available data, such as places of interest (e.g. places of worship), as that can be considered to infer either religion and/or race. If such statistics are needed for determining factors and/or causes in ascertaining a hypothesis, then these intentions need to be disclosed to the data subject beforehand. (Pulkkis et al. 2018)

We can assume that the invasion of the data subject's privacy is a measurable property and not a binary value (cf. RQ1 & RQ3). The measurable property can be an objective opinion of the courts or data protection supervisors, for example as in the case Google v AEPD and Costeja (Case C-131/12). The recommended approach is that it is a property determined through a subjective opinion of both the data subject and the controller. Determining a level of privacy violation or even the risk, may be challenging. Particularly when processing is done based on public interest, as in the case of a search engine, it may be difficult to determine potential privacy violations. Private legal entities that control platforms that utilise the argument of processing based on public interest face deeper scrutiny by data protection supervisors and may additionally face national laws that limit such processing further.

When data are shared in the form of a message that is intended to be read by a group of people outside the immediate family, it becomes difficult to argue that data have not been shared manifestly. Once data have been shared manifestly by the data subject, the GDPR considers that the data have lost its private property (cf. RQ1). This applies also to personal data categorised as special. Furthermore, the fundamental human rights given by the EU charter, offer protection for personal correspondence that should be considered to include messaging services such as

email and SMS. When it comes to messaging between many-to-many participants (e.g. instant messaging groups) the argument of invasion of privacy to the data subject may be considered weakened. Provided that a preponderant interest of the public exists and can be shown, then processing of personal data may be allowed without the consent of the data subject. In case personal data have not been manifestly shared by the data subject himself, such processing (incl. that of public interest) can be challenged on the basis of invasion of privacy.

Tracking users on the Internet has become an important part of driving new sales. Service providers want to identify individuals among a myriad of devices and this can be performed by using a combination of techniques, but at the centre is often a global social media platform that requires the user to login to its service (cf. RQ3). Techniques such as browser or device fingerprints, location segmentation, traffic meta-data and different types of beacons (incl. audio) can be combined to ensure detailed tracing of users. Today tracking concerns a broader spectrum of details than linking data to a natural person. To gain an in-depth understanding of the environment in which users live, companies attempt to understand the context of the environment. A user is thought to be more easily persuaded in a certain context compared to another context. To determine the physical context the user currently resides in, ultrasonic cross-device tracking may be used (Arp et al. 2017). The cross-linking may be achieved through active apps, and ultrasonic beacons emitted from, for instance, TV programming, store devices, or websites. This type of technology should in general be considered prohibited in the EU without specific consent by the data subject for the use of such profiling services (cf. RQ1 and RQ3). In practice, the device will be able to listen to any audio signal, including speech, without the subject's knowledge, and any personal data recorded ought to be considered special category data. However, there are legitimate reasons for using similar technology. Digital personal assistants (e.g. Amazon Alexa) may employ similar technology to deliver prescriptive insights to users. As any profiling based on special category personal data requires specific consent, such operators may need separate consent for suggesting commercially driven suggestions, such as 'recommend that you get product A from Store X because it is on sale', compared to need-based suggestions such as 'remember to get X on the way home as your Y (e.g. fridge) is empty'. When a child uses a digital personal assistant, the question becomes what happens if the parent has not consented to the processing of the child's voice or commands. Does this require the service provider to try to detect who is talking and predict what age the subject is? When considering children's use of apps and the Internet in general, the use of identification mechanisms should be developed and required by law. An example given of such lightweight mechanisms is through a dedicated HTTP header attribute.

Based on sub-section 4.2.4 and 4.2.6, we can draw the conclusion that a provider of intelligent services will face the least amount of scrutiny from the regulator if

client-side processing is performed (cf. RQ1and RQ3). Decentralised solutions that only utilise local storage may perform processing quite freely; the primary exception may be special category personal data that would require a specific processing consent. The local storage may be backed up on a central node if encrypted by the user. This would allow the controller to claim that personal data are not used in processing, and that the virtual identity of the user is not naturally identifiable. Client-side processing may also be more secure as data would only be stored in a readable format locally (cf. RQ2). This will require a certain amount of processing power from the client device, but assuming Moore's law holds, then this challenge can soon be trounced.

Talk is cheap. Show me the code.

—Linus Torvalds

5. Security in Information Systems

The GDPR requires controllers to safeguard that personal data is processed in a way that ensures appropriate security. The direct incentive used to compel companies to invest in security is the potential fine if found in breach of the GDPR. The GDPR as established in chapters 3 and 4, focuses on a methodological approach to reduce the risk and scope of security incidents. The risks identified by the GDPR include protection against unauthorised or unlawful processing, accidental loss, destruction, or damage. The solution for achieving this is stated as using appropriate technical or organisational measures. To assess the appropriate level of security, account shall be taken of risks presented by data processing (GDPR 2016, art. 5(1)eb; art. 30).

The e-Privacy Directive (art. 4) calls attention to providers of publicly available electronic communications services and that they must take appropriate technical measures to safeguard security of its services, with respect to network security. Although from a technical perspective any Internet based service involves the communication of data over a public network, the e-Privacy directive is much narrower in scope. The e-Privacy directive applies to providers such as traditional telcos and ISPs, but likely also to some Over The Top (OTT) providers, i.e. providers of one-to-one messaging apps, e-mail platforms, and VOIP services.

The Directive on Network and Information Security is similarly limited in its application (cf. sub-section 3.1.1), as the NIS concerns the security for operators of essential services (e.g. utility platforms of a considerable public interest) and for digital service providers. Digital service providers are listed as such organisations that provide online marketplaces, online search engines, or cloud computing services (NIS, recital 15-17). Other digital service providers are thus not bound by the obligations laid out in NIS, but the law can be seen as best practice for the industry. Some of the obligations listed are:

> preventing risks – technical and organisational measures that are appropriate and proportionate to the risk,
>
> ensuring IT security – ensure a level of security of the network and information systems appropriate to the risks,
>
> handling incidents – prevent and minimise the impact of incidents on the IT systems used to provide the services. (Pulkkis et al. 2018)

The GDPR does not define a certain required level of security, but rather it implies that whether an appropriate level of security existed shall be assessed later on. This advocates also that what will be considered an appropriate level of security will likely change over time. The approach can be considered in line with the Regulator's aim to create a technology agnostic law. However, determining technological actions based on achieving an environment that ensures appropriate security, based on the risks listed above, may be challenging for controllers,

processors, and owners of information systems (cf. RQ1 and RQ2). The regulators focus on data security methods (e.g. data minimisation and privacy-by-design) is understandable, but from a technical perspective appropriate network security is just as important. The omission of what can be considered guiding network security principles in the GDPR may lead to a lesser focus from companies on improving this aspect of their information systems (cf. RQ2 and RQ2.1). Thus, this chapter will focus on documenting researched solutions to data protection problems that arise from network security issues. An additional benefit of developing and defining state-of-the-art methods available at the time of writing and connecting them to the Regulation, is that these can become important metrics for the judiciary system and for jurisprudence reasons.

This chapter presents three exploratory single-case mechanism studies (Wieringa 2014) to determine available security measures against network threats a company faces when handling personal data (cf. RQ2 and RQ2.1). The review is not intended to be exhaustive, but focus on two state-of-the-art techniques that are further elaborated in two of the papers included (Xiang et al. 2014; Paarnio et al. 2015). The techniques are of importance in determining what constitutes using appropriate technical security measures, as set out by the Regulation (GDPR 2016, art. 5(1)eb; art. 30). A secondary objective with the chapter is to understand the technology stack and methods behind big data analytics, as well as to elaborate the design issues and certain attack vectors (cf. RQ2.1). The realisation of an architecture for a big data analytics processing tool was expounded in the paper Westerlund et al. (2014).

5.1. Big Data Analytics Technologies

In 2012, the Cloud Security Alliance initiated a Big Data Working Group with representatives from industry and academia. The agenda for the group was to be a conduit for highlighting the importance of developing big data methods and tools for information security. In a report issued by the Big Data Working Group (2013), they exemplify big data analytics approaches to information security. One important tool for implementing big data analytics solutions for network security is Hadoop. Hadoop can be described as a distributed database. Hadoop was the first widely used open-source system to implement and extend a distributed MapReduce programming model. The processing capabilities of Hadoop are built upon the Hadoop Distributed File System (HDFS). The HDFS is a general-purpose file system, which is designed for handling file sizes up to terabytes and hundreds to thousands of processing nodes. Supported file formats are such that have a built in schema support, e.g. various types of UTF-based text files. HDFS does not support binary formatted files in general, but offers end-to-end encryption of data read from

and written to HDFS[28]. The best processing performance is achieved when available jobs can be scheduled to an equal number of processing nodes. However, a distributed architecture also tends to have an overhead from network communication, meaning each node should have a sufficiently large amount of data to process. Enabling encryption may have a detrimental effect on processing performance. End-to-end encryption ensures that sensitive data can be stored and processed securely though, provided encryption keys are not compromised. Attack vectors do exist that may make the processing unsecure, which particularly affects cloud installations when the cloud provider cannot be trusted. If an attacker gains root access to data nodes or name nodes, such malicious root users may also gain access to the in-memory state of the processes holding encryption keys and data in clear text[29]. This issue has, inter alia, a relevance to the negotiations regarding third country data transfer frameworks, for instance between the United States and the European Union over a safe harbour framework and its successor the Data Privacy Shield. The European Commission's Decision (2000/520/EC, of 26.07.2000, art. 1[30]) considered there was an ensured adequate level of protection for personal data transferred from the EU to organisations established in the United States. In the case Schrems vs. Data Protection Commissioner, the European Court of Justice issued a judgment declaring the European Commission's Decision as invalid. According to the judgment, "*the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments*" (Case C-362/14, point 97). Consequently, if the cloud provider maintains root access to nodes, inter alia for national security reasons, then the use of Hadoop may be considered unsecure for storing personal data. This issue is not limited to Hadoop, but rather describes the challenge of cloud computing software in general (cf. RQ2 and RQ2.1). The data transfer agreement framework has since been replaced by the EU-U.S. Privacy Shield [31], but its legal validity is still questioned and the technical challenges with cloud services that handle personal data remain much the same (Lynch 2017).

---

[28]See HDFS Data At Rest Encryption. Accessed 30.07.2016, https://www.cloudera.com/documentation/enterprise/5-4-x/topics/cdh_sg_hdfs_encryption.html

[29]For further details, see Cloudera's summary on HDFS Attack vectors. Accessed 30.07.2016 https://www.cloudera.com/documentation/enterprise/5-4-x/topics/cdh_sg_hdfs_encryption.html#concept_db3_d3w_hp

[30] See Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. Accessed 30.07.2016 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

[31] See European Commission - Press release, European Commission launches EU-U.S. Privacy Shield. Accessed 05.09.2017 http://europa.eu/rapid/press-release_IP-16-2461_en.htm.

Through the MapReduce programming model, Hadoop offers developers a rudimentary interface for manipulating data. On top of this interface, numerous tools that consume said interface, but which offer the developer more elaborate ways to manipulate data exist. The ease of use in distributing data among processing nodes is an important feature of the tool. Hadoop has two main layers, MapReduce and HDFS. HDFS, as earlier stated, is a general-purpose file system, meaning its intended use is to store data, i.e. historical data or data-at-rest. This data are then automatically distributed among the data nodes by HDFS. An implication for the developer is that it becomes difficult to work with real-time transactions (streams), as they would need to be stored and indexed first, in the file system. Many of the tools built on top of the Hadoop platform could at the time of writing still not handle streamed transactional data. Section 5.2 presents an implementation of a supervised machine learning algorithm on top of the Hadoop platform.

Before the public release of the Hadoop platform, we set out developing our own architecture in order to understand how a real-time transactional platform operates and to explore any limitations. The challenge of dealing with temporally structured data is a common data science problem in industry, e.g. developing Internet of Things services, user profiling, network security analysis, or financial services. Dealing with streamed transactional data using machine learning algorithms, requires that historical data be used for training and real-time data for prediction. Achieving a generalised architecture for handling both scenarios became our main aim. The secondary aim was to automate the machine learning process, so that once started there would not be the need for interference from an operator. This was a challenge as machine learning models often tend to be fairly sensitive to issues such as model overfitting in training (i.e. a model begins to memorise training data rather than generalising) and model specialisation (i.e. a model only works well on part of the data) (cf. RQ1). To solve this issue, we decided to implement the use of ensemble models (i.e. a combination of many models) as well as continuous model quality assurance. For processing that falls under the GDPR, detailed efforts must be made that avoid situations where faulty model outputs/decisions are provided to data subjects (RQ2.1).

5.1.1. Developing a Generalised Scalable Software Architecture for Analysing Big Data

The initial training process is always pre-determined as batch processing by the system user when defining the model setup. As the requirement on our system is to be able to handle both data-at-rest and real-time data, we mapped two separate workflow processes: model training workflow and live prediction workflow. Our definition of the workflow for training the models is seen in Figure 1. The workflow for the real-time prediction is seen in Figure 2.

In the model training workflow, data (accessed from the Data Gateway) have been pre-processed for validity and other preformatting techniques such as adjusting for required granularity, i.e. time resolution. The data feature extraction block refers to techniques such as component analysis, standardisation, normalisation, or any ad-hoc technique as required by the developer. While data are being prepared, an asynchronous flow initialises contact to the worker nodes in the public or private cloud (hereafter referred to as *cloud* when no differentiation is needed). These worker instances will be started manually, as to determine resource availability, with a pre-prepared operating system image containing required software (e.g. correct software versions, security and our base client service that starts automatically with the instance), in order for the system user to have full control over all simultaneously running instances. Once the initial handshake is performed, the necessary binaries defined by the developer and used by worker instances to process data are transferred to the worker nodes. We refer to these binaries henceforth as *software agents*. The software agents automatically subscribe to the worker instance monitoring service in order to receive jobs, including setting up the model. The differentiation between model, agent, and worker instance is that the worker instance represents the virtualised cloud instance (including our base client service). The model is the serialised machine learning model representation. While the agent is a generic binary with the ability to report status, listen to data events and execute models as defined in the data event. A data event refers to a new or updated input variable; however, the actual data packages sent to the worker instances vary depending on the type of job. In the case of a training job, the data package includes all the input data a model needs in a fully pre-processed format as well as model metadata. The input data for training can be of considerable size and is therefore transferred in a compressed format from the data gateway to the worker node. Data in the training process are therefore transferred in a binary format, and communication is encrypted over HTTPS/TLS.

An important part of data security in the GDPR is data provenance, i.e. authenticity and integrity of data used for analytics. An aim is to investigate ways to achieve data integrity for model output as well, which can also be transferred to a production-level system (RQ2.1). The training process is thus fully automated and we achieve this by making use of both a verification dataset and an evaluation out-of-sample training dataset for calculating model error rate. The verification dataset is usually a pre-training data sample. Training continues until the software can confirm that a certain training iteration (epoch) delivered the lowest in- and out-of-sample training error, in order to minimise the risk of overfitting. We perform a comparison of the verification error and training error to determine the convergence point, when they combined reached their minimum. Once the model training is considered to have reached its minimum training error or timed-out, we perform a second out-of-sample test, referred to as evaluation, of the best iterations

found using data from post in-sample data to determine the model's most recent performance and ultimately which training iteration to choose as finalised model.

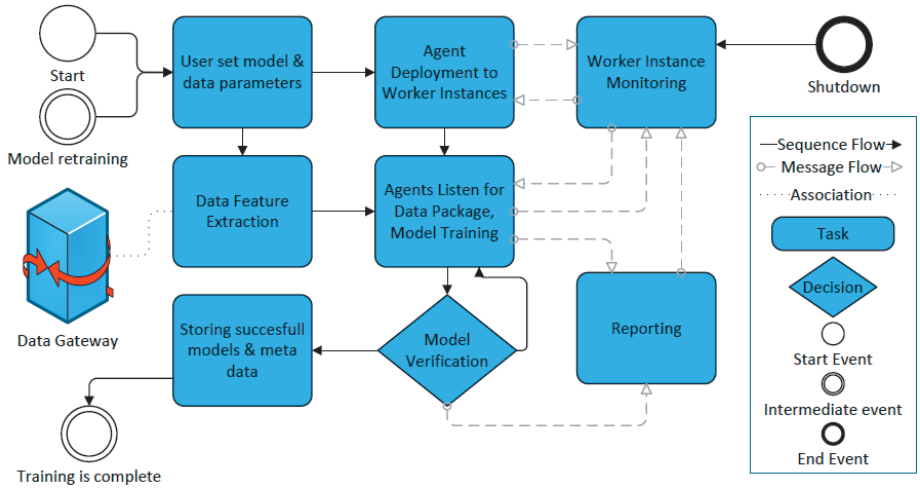


Figure 1 - Training workflow (Westerlund et al. 2014)

Once the system has trained the models and the system user has initiated that real-time forecasting should commence by choosing a certain model set (ensemble) to be deployed and starting the software agents, the jobs are distributed randomly among the available software agents. To achieve this, we implement a queue of jobs (i.e. new data events) that are sent along to software agents that indicate they are free. Jobs become outdated once the point in time they are supposed to be forecasting to has passed. In case the queue contains jobs that are outdated, which implies we have a performance bottleneck, the job is cancelled automatically. A data event during real-time prediction includes, in addition to the input data (data transaction) needed for prediction, network weights and metadata required for processing. For live prediction, data events are normally not compressed as the compress/decompress cycle would not be efficient for a minuscule dataset such as the envisioned data event.

Once a job is processed, the result is collected centrally for both calculating a new ensemble vote as well as to determine if a certain model has been performing badly and needs to be retrained. For automation purposes (i.e. not requiring human intervention during training, live prediction and model retraining), we consider using an ensemble of models as a requirement. This technique is also known as voting by committee. There are several techniques for calculating an ensemble vote; we chose to use out-of-sample evaluation data for determining the initial relevance of each model. This allows us to later evaluate each model's continued performance in regards to its recent forecast and based on the evaluation error rate to determine its current voting rights.

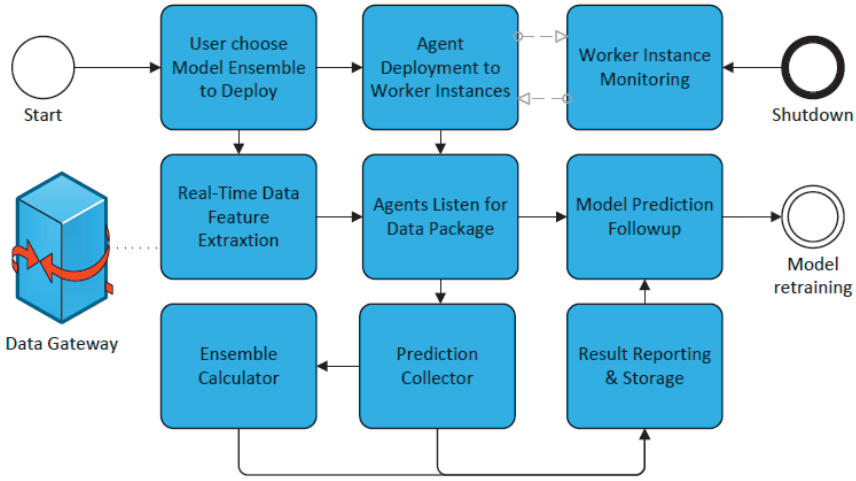


Figure 2 - Live prediction workflow (Westerlund et al. 2014)

The proposed architecture is illustrated through a system component diagram, Figure 3. There are three separate components; the agent, the server and the client. The client component allows the system user control over model training and execution, as well as management of cloud instances. The client takes the form of a graphical user interface. The server component acts as a central node responsible for interfacing with the client component, extracting features from data sources, maintaining efficient distribution of new jobs, and collecting and processing of modeling forecast results as defined. The third identified component is the agent, responsible for performing the jobs provided by the server component. As our aim was to create a unified design for both the training process and live predictions, we achieve this through polymorphism and the extensive use of externally available Application Programming Interfaces (API) and internal interfaces between the components and sub-components respectively. One of the challenges faced was to solve how feature extraction is handled, here defined as *data generator*, in both cases. To perform feature extraction on both historical and real-time data with the same underlying algorithms requires that data be formatted using predetermined data tuples, which include a required amount of data elements and using the same time resolution. For certain algorithms, e.g. normalisation algorithms, previous scaling values used for historical data must be employed during real-time prediction as well. These types of values must therefore be stored as model metadata during training as they are used during real-time prediction as well. In our architecture the data generator and decision calculator were designed as internal sub-components of the server. In case the processing demand should exceed the resources available on the server, these two components can be external by executing on separate processing nodes. This architecture should mitigate some of the challenges when using non-linear methods in the design of intelligent systems (cf. RQ1 and RQ2.1). The set-up

offer ways to improve data integrity for analytical modeling output that is horizontally scalable and may offer high quality results.

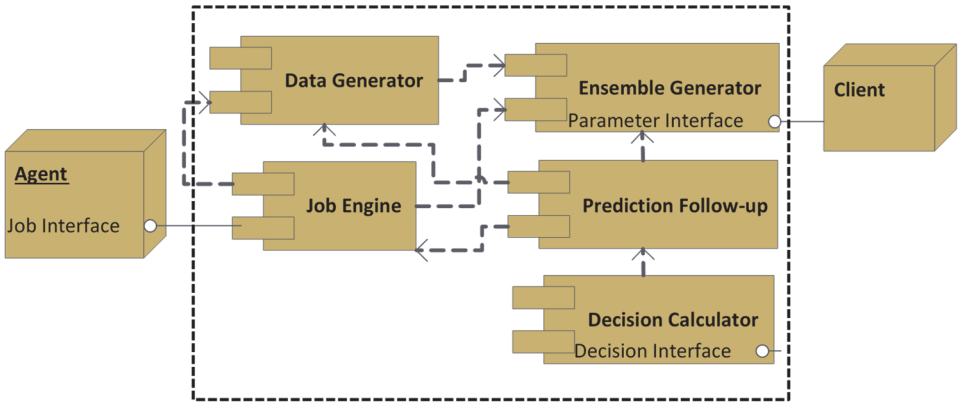


Figure 3 - System component diagram for proposed architecture (Westerlund et al. 2014)

5.1.2. Security Risk Assessment

Defining and implementing a secure system architecture is always important and challenging. By performing a risk assessment and prioritising the type of security risks one wants to avoid, it is possible to define the security objectives of the system (Savola et al. 2012). The risks identified with highest priority to our system were unauthorised access to the system, exposure to physical attacks and malicious resource consumption. Therefore, our main security objective is to avoid financial exposure of an attacker being able to highjack our account resources to run their own services. Consequently, we employ the following security controls:

1. Each system user is required to use a personalised cloud account.
2. System passwords required for instance control are only entered during runtime (through a secured remote desktop connection).
3. Communication between instances is always encrypted over HTTPS/TLS.
4. Each instance is required to use a certificate that is unique for each system user.

This type of risk assessment must always be performed on an individual and ongoing basis. Noting, that if the system is to be handling sensitive data (e.g. personal data), then protecting that data from possible exposure should be a prioritised risk. Our risk assessment did not include such a requirement; therefore, we omitted end-to-end encryption and pseudonymisation of data. Communication is encrypted between nodes and node access is defined through personal certificates, but data is stored in a raw format. As in the Hadoop case, implementing end-to-end encryption for our proposed architecture would still make it sensitive to a malicious

root user. However, provided the cloud operator allows the use of a custom cloud instance, which can be sufficiently hardened, this would potentially be an improvement compared to the use of X as a Service (XaaS). The inability for XaaS customers to provision the underlying environment and root access to nodes in XaaS, may make the environment more unsecure. In addition, any vulnerabilities in the hypervisor layer, i.e. the layer that cloud instances execute upon, will be a serious attack vector. [32] [33] This applies particularly to advanced persistent attackers, such as state-sponsored hackers.

5.2. Network Intrusion Detection Using Machine Learning

Traditional network security focuses on what can be considered passive techniques. Such techniques are for instance authentication based on a login/password combination, static firewall rules, and static network separation. Although these methods provide important means for creating a company backbone, they are always based on a binary trust-relationship, to provide 'good users' with access and keep 'bad users' out. The inability for passive systems to continuously re-evaluate and adapt the trust-relationship when for example user credentials are leaked or zero-day vulnerabilities are utilised, is problematic. Passively secured systems offer relatively little protection once the system breach has occurred.

The introduction of big data analytics tools into the network security workflow offers great possibilities for detecting intrusions or unauthorised data access (cf. RQ2 and RQ2.1). Although the GDPR mostly consider regulating internal data processing for business purposes, keeping personal data safe from unauthorised use, be it from an internal or external perpetrator, is just as important. The ability to employ machine learning algorithms by using big data tools for detecting intrusions in a network environment is important. The amount of network data to be analysed has been growing rapidly and to be able to perform network intrusion detection using machine learning requires a massively scalable system. Although intrusion detection has been a hot research topic since the late 90's, the utilisation of research methods in industry has been rather slow. One of the main reasons for this has undoubtedly been the cost of processing network data. A network is often customised to a certain company need, and hence an active network security intrusion detection system, based on some type of analytical model, may have to be trained using on-site data. The use of machine learning in detecting network intrusions is important, as other methods such as rule-based detection tend to deliver results that can be circumvented through the exploration/estimation of such rules by an attacker. In addition, the creation of rules often requires human expertise

[32] For a detailed survey of cloud security issues, see Modi et al. (2013).
[33] For hypervisor specific attack vectors, see Perez-Botero et al. (2013).

of known threats in the creation process. The use of machine learning in the process may improve generalisation and thereby improve detection of unknown threats.

By making use of a de-facto standardised dataset, KDDcup99, we present a machine learning method that scales horizontally without losing detection accuracy for classifying intrusion attempts. We employ a machine learning algorithm called Extreme Learning Machine (ELM) (Huang et al. 2006) implemented on top of Hadoop's MapReduce programming model. The purpose of our MapReduce implementation of ELM is to determine that it scales horizontally and that it can be used for network intrusion detection (cf. RQ2). Using the MapReduce programming model, we show that machine learning based intrusion detection using ELM can extend its applicability to significantly larger datasets than the KDDcup99 dataset. Provided enough computer resources can be allocated to the processing tasks, growing the dataset is possible without increasing training time drastically, due to the near linear scaling ability of the proposed ELM algorithm[34].

We perform two kinds of intrusion detection experiments; binary intrusion detection and multiclass intrusion detection. The experiment evaluates MapReduce ELM against a local implementation of ELM. For each experiment, we compare two characteristics of MapReduce ELM with local ELM. The first characteristic focuses on processing performance evaluation of MapReduce ELM against the local ELM. The second characteristic compares the performance of the local ELM and MapReduce ELM by model accuracy. To determine the accuracy the local ELM is tested on one standalone machine and MapReduce ELM on a cluster of 10 nodes. Both models were trained with datasets of varying size. In each experiment, we recorded the following information:

False Positives (FP) – the number of normal instances detected as attack instances

False Negatives (FN) – the number of attack instances detected as normal instances

True Positive (TP) – the number of correctly detected attack instances

True Negative (TN) – the number of correctly detected normal instances.

For each training dataset we repeated training and testing 4 times in order to obtain averages of FP, FN, TP, and TN. Based on these results, the performance of MapReduce ELM against local ELM was measured by Overall Accuracy, which means the percentage of correctly detected sample instances.

5.2.1. Performance Analysis of Binary Classification

For the binary intrusion detection experiment, we pre-processed the training and testing datasets by giving label value 1 for each normal sample instance and label value -1 for each attack instance. Overall Accuracy for both MapReduce ELM and local ELM

[34] For a detailed description of the construction of the algorithm, see Xiang et al. (2014).

is about 93% or better depending on the training set size, see Table 3. A slight Overall Accuracy improvement is achieved by increasing the size of the network (i.e. number of hidden neurons from 50 to 200). MapReduce ELM has a fractionally higher detection rate than local ELM in almost all training dataset experiments. For a larger training dataset size, Detection rate increases slightly as well. False Alarm rate is low, between 0.89% and 1.72%, in all training dataset experiments.

Table 3 - Intrusion detection accuracy for ELM with 50 hidden neurons (adapted from Xiang et al. 2014).

N	accuracy binary		accuracy 23 classes	
	local	map reduce	local	map reduce
100k	94.75	94.65	92.86	92.78
200k	93.31	94.57	93.26	93.91
300k	97.08	96.6	95.16	97.28
490k	97.58	97.7	96.84	97.41

Efficiency analysis of MapReduce ELM compared to local ELM was performed with three different dataset sizes 1M, 2M, and 3M samples, using a network with 50 hidden neurons. For each dataset, the program was executed 4 times on a single machine (local) and on 15, 20, 25, and 30 cluster nodes (MapReduce) to calculate average execution times. From Table 4 we can see that MapReduce ELM can significantly decrease the execution time compared to local ELM. The comparison could not exceed 3M samples due to that the local ELM ran out of memory after 2M samples. The execution time of MapReduce ELM decreases as the number of nodes increases up to 25 nodes. When increasing the number of nodes from 25 to 30, the running time increases a bit because of increased communication between nodes. We noted a drawback of the MapReduce framework in the overhead required by the disk read/write operations of each map/reduce task. This overhead can prolong the execution time if the response time of the hard disks cause the workload on the processing nodes to be delayed, i.e. workloads are as a result inefficiently processed.

Table 4 - Execution times (in seconds) of MR ELM for binary class intrusion detection with 50 hidden neurons (adapted from Xiang et al. 2014).

number of nodes	dataset size N		
	1M	2M	3M
single	6659s	11837s	Out of mem.
15	278s	441s	643s
20	258s	400s	558s
25	223s	332s	462s
30	246s	382s	470s

5.2.2. Performance Analysis of Multiclass Classification

The training and testing datasets for multiclass classification was pre-processed by assigning an additional feature for five class values (labels), one label for normal group and 4 labels for main attack groups. A second added feature includes 23 class labels, 1 label for the normal group and 22 labels for specific attack types. We use these added features for designing two different experiments. The 5-class and the 23-class experiment denotes that the model output has an equal amount of output dimensions. For both the 5-class and the 23-class experiment, MapReduce ELM and local ELM have a very similar and relatively good Overall Accuracy above 90% (see Table 3 for 23 class accuracy). For an increased training dataset size, Overall Accuracy increases. For the largest training dataset size, Overall Accuracy is slightly improved by increasing the number of hidden neurons from 50 to 200.

Efficiency analysis of MapReduce ELM (see Table 5) shows the execution time of MapReduce ELM for three different dataset sizes in multi-class intrusion detection with 50 hidden neurons. The experiment was performed using three dataset sizes by applying the same test protocol as in binary classification. The results are similar to binary classification. MapReduce ELM significantly decreases the execution time in comparison with local ELM. Increased communication between nodes slightly increases the execution time of MapReduce ELM, when the number of nodes is increased from 25 to 30. The speedup is approximately linear except for the tail. From 15 to 25 nodes, regardless of input sample size, the increase is near linear as more nodes improve parallel computing ability. Increasing the number of nodes from 25 to 30 decreases speedup because of the increased overhead in nodes mainly caused by communication between nodes.

Table 5 - Execution times (in seconds) of MR ELM for multi-class intrusion detection with 50 hidden neurons (adapted from Xiang et al. 2014).

number of nodes	**dataset size N**		
	1M	2M	3M
single	7336s	13498s	Out of mem.
15	294s	485s	659s
20	256s	431s	571s
25	230s	367s	488s
30	252s	382s	494s

5.2.3 Result Outcome

We consider our Overall Accuracy good, considering that we did not perform elaborate data preformatting or use highly optimised modelling techniques (e.g.

parameter tuning or ensembles). Our aim was to use a standardised modelling technique, with minimal human expert knowledge of the dataset or model, to determine whether more data can be used to improve classification, and if horizontal scaling works on a complex dataset, compared to a local implementation. For both research questions, we consider the aim achieved.

Implementing an active network intrusion detection system based on machine learning techniques offers companies today a relatively rapid way to improve security in their networks (cf. RQ2). Using an open-source big data solution offers a cost efficient way to improve security. The workflow demand is initially perhaps not to detect intrusions in real-time, as a technique described in section 5.1, but rather as a resolution defined as near real-time and applying 30-second to 1-minute segment intervals may suffice. This requirement would be system dependent; a system with multi-layer security may be less sensitive to information loss if the outer layer is breached. Hence, multi-layer security may provide system administrators with more time to collect and then process network security data, possibly for a higher overall accuracy detection. Another processing tool, Apache Spark, built on top of Hadoop's HDFS file system can perform detection with such segment intervals. Spark offers an improved programming environment and includes in-memory computing on data nodes. In-memory computing should improve processing efficiency, since data does not have to be stored on the file system after each task, which we found to be a bottleneck with Hadoop MapReduce. An additional benefit from using the Hadoop platform for intrusion detection is that it offers a relatively resilient and cost-efficient mass storage of historical data. Provided a company stores its forensic network data this way, it will in the forensic process be important to determine what happened or to build an improved training dataset that includes new types of intrusion threats.

An insight gained during our research is that the main challenge companies will likely face, is in determining what data should be recorded and how to label the training set to create a detailed and specific representation of potential threats the individual system can face (cf. RQ2 and RQ2.1). Current rule-based intrusion detection tools can be used as a first step in generating a company specific dataset. Iterating based on such a dataset can then lead to the identification of new threats through the generalisation ability of a machine learning model. In addition, through organising a company hackathon, new training data can be amassed and labelled. Another approach for collecting valuable data for a content management system (web application) is examined in section 5.3.

5.3. Active Intrusion Management for Open-Source Software

Today, a common breach of user data often arises from an intrusion attack by a hacker on an information system. Software with public communication endpoints, such as an application implemented on top of a web server, tend to offer intruders

an important attack vector. Open-source software is often hailed for its security enhancing ability in comparison to proprietary software. This is based on the assumption that many others than the original coder have vetted open-source software. However, open-source software also offers an important additional attack vector for hackers. So-called zero-day vulnerabilities are undisclosed vulnerabilities in a system that someone has found, but still exist as a flaw, i.e. yet to be fixed in the system. This allows an attacker, potentially, to use the exploit without a system administrator being able to detect the intrusion with traditional passive network security means. Open-source software allows the hacker to examine the source code and test any multitude of attack vectors in order to gain privileged access to the system, before commencing an attack on the intended target. In many cases this may make the footprint of the intrusion too small to detect. An additional problem is the mixed used of open-source and proprietary software. Modular open-source software that allows for customisation through proprietary plugins may be problematic if the quality assurance process for the proprietary software is limited in scope.

We present an initial methodology in extension of current recommended methods for securing WordPress software[35]. The challenge is to go beyond the installation procedures often used today, and propose ways for hardening an installation of the most popular Content Management System (CMS) WordPress. WordPress is an easily extendable system, and as a result numerous plug-ins, which the original developers of WordPress do not control, exist [36]. According to independent statistics, WordPress powers 25% of all websites worldwide, while the two closest competitors, Joomla and Drupal combined are used by 4.9%[37]. As later will be shown, these plug-ins are sometimes extraordinarily easy attack vectors for a potential intruder. This situation has arisen from bad software engineering practices (e.g., lack of quality assurance for plug-ins), and the ease of use (in-depth technical skills are not required for installing and using the software). A potential attacker can automatically scan the Internet (IP addresses and ports) for public installations of the software and their corresponding vulnerabilities with minimal risk to be detected as a threat. We consider current passive intrusion management methods often too limited in ability to secure installations, as current defence methods as firewalls, antivirus software and current intrusion detection systems (IDS) can often not detect these intrusions. We examine the research question as how to define "appropriate security" (cf. RQ2) through the hardening of an

[35] For best WordPress administrative practices, see https://codex.wordpress.org/Hardening_ WordPress. Accessed 30.07.2016.
[36] It should be noted that not all plug-ins are open-source, and our methodology should also encompass these closed-sourced plug-ins.
[37] For more details regarding the CMS study, see https://w3techs.com/blog/entry/wordpress-powers-25-percent-of-all-websites. Accessed 30.07.2016.

installation of WordPress and the creation of an active intrusion detection methodology for the WordPress system.

5.3.1. Active Defence

We define active intrusion detection as the process when both intrusion responses and forensic investigations are proactive and/or automatically triggered by intrusion attacks. We present a method for creating what we refer to as booby traps for web software. Crane et al. (2013) define booby traps as "*code providing active defence that is only triggered by an attack*". A booby trap neither implements program functionality nor influence its operation. The idea is based on that the program is unaware of these booby traps, and therefore unable to trigger them. An attack who may be scanning the software will by mistake end up activating one of the traps. Once a booby trap is triggered the software, or rather the intrusion detection system, will immediately know that an attack is under way. Crane et al. (2013) focused on automatically inserting booby traps into the original program code during compilation or program loading. In our case, we examined web software and found that inserting booby traps automatically during the software installation process makes more sense. The use of booby traps in software can allow the system to perform advanced forensics to identify an attack in real-time, to facilitate a deceptive response, or a denial of access response.

A tool often used by network security professionals is a honeypot, an unsecure system that is used to draw in hackers. A honeypot does not expose any real system but functions as a decoy to draw in attacks so that the patterns attackers used can be forensically examined. An exploit can be honey-patched, which means that the system administrator concerned is aware of said exploit, but instead of only patching the exploit, the system also redirects any attempt to use the exploit to a parallel system with an unpatched exploit. This offers system administrators the ability to continue tracing a potential intruder and forensically analyse data that is left behind. The Linux distribution Active Harbinger includes many tools for active defence, e.g. against network scanning and restrictive access to certain services. These are important tools for network security professionals, but offer limited help for the layman or novice that often employs WordPress installations.

5.3.2. Return-oriented programming attack on executables

In Paarnio et al. (2015), we present a technique against code-reuse intrusion attacks that are based upon similar principles to return-oriented programming (ROP) in executables. Return-oriented programming attacks signifies when an attacker takes over program flow control in a network connected computer. This type of attack takes place without injection of malicious program code, which makes the attack very difficult to detect. In an executable, a return-oriented programming attack is

achieved by manipulating the control stack address of a RETN (return from procedure) instruction. By manipulating the address, the attacker can choose what to execute next. The attack is implemented by execution of a gadget chain. A return-oriented programming attack is achieved by exploiting some buffer overflow vulnerability that starts with an injection that overwrites program code including the RETN control stack address. Once a new RETN address is inserted, the program flow can be diverted to execute an attacker-defined gadget chain. (Prandini, and Ramilli 2012; Roemer et al. 2012)

To booby trap an executable as an active defence method, a similar method to return oriented programming for attacking purposes, can be employed. By inserting defensive gadget chains, which disrupt program flow if executed, they may catch scanning of or unintended execution of calls in binaries. During compilation or program loading, the binary is manipulated by inserting randomly return-oriented programming gadgets into the assembly code, including implementing a technique called Address Space Layout Randomisation (ASLR). The Address Space Layout Randomisation technique changes instruction addresses randomly. As earlier stated, the normal program flow is not aware of the existence of the booby trap gadgets and can therefore not trigger them. Address Space Layout Randomisation can also change the binary structure, in order to create place for the booby traps. If an attacker then scans for access points that have been replaced by the insertion of a booby trap, the booby trap will be triggered. Once a booby trap is activated, it can send an alert to a system administrator or an intrusion detection system. Figure 4 illustrates how the binary is modified for the insertion of booby traps, by moving gadgets around.

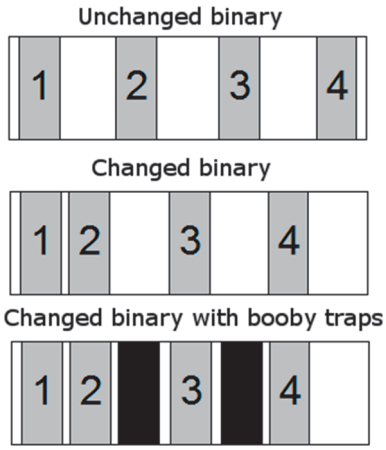


Figure 4 - Booby trap modified executable (Paarnio et al. 2015, reprint with permission)

5.3.3. Booby trapping web software

The basic concept of return-oriented programming attacks/booby traps described for executables does not extend directly to web applications. However, application code running on a web server can be booby trapped by modifying the source code. Since the source code is generally not pre-compiled, it can be modified while being installed or at a later stage, once a vulnerability has become known.

The initial step in our study focuses on known vulnerabilities, which are first patched manually and then booby trapped. A potential intruder should be unaware of the fact that the patch has been applied. A hacker often uses either a passive or an active analysis of installed plug-ins[38]. Passive analysis focuses on detecting specific plug-ins and their vulnerabilities through regular valid HTTP requests, while active analysis entails automated scanning to perform hundreds or even thousands of mostly invalid HTTP requests. A booby traps function can then be to register forensic information once the hacker's analysis identifies the target and the attack begins.

One of the examples provided in Paarnio et al. (2015) is an exploit for the plug-in WordPress Wp Symposium 14.11. The plug-in version includes a vulnerable file UploadHandler.php that accepts as upload any type of file, which means that a malicious shell code file can be uploaded. An exploit script is publicly available that creates a backdoor to protected files on a WordPress site by simply uploading a shell script[39]. The exploit allows a script that is uploaded to the server to be called by a user, by placing a direct request to said file, with the result that the script will execute with web server privileges. The attacker can then execute arbitrary executable code on the web server. The vulnerability can be patched by only accepting an upload of certain file types. While applying this patch and inserting a call to a booby trap, data on anyone who tries to make use of the exploit as well as any script they try to execute remotely can be gathered in a log.

Manually booby trapping all plug-ins installed on a typical WordPress installation was found to be both labour intensive and error prone. This approach captures only publicly known vulnerabilities. As the potential intruder should be unaware of patches applied, it also becomes difficult to manage as the client can often detect software version updates on the server. Therefore, a sophisticated attacker would be able to determine a likelihood of success for an attack before commencing.

---

[38] For further information attacking WordPress, see https://hackertarget.com/attacking-wordpress/. Accessed 30.07.2016.

[39] For further information see C. Viviani, WordPress Wp Symposium 14.11 - Unauthenticated Shell Upload Exploit, http://www.exploit-db.com/exploits/35543/. Accessed 30.07.2016.

To improve the ease of capture and mitigate the effect of attacks we develop two novel approaches: redirecting requests for missing resources and path randomisation for installed resources.

5.3.4. Redirecting Requests for Missing Resources

When an attacker performs active analysis, a website receives requests for a large amount of potentially unknown or missing resources, e.g. files that belong to plug-ins that are not installed on the system. These requests are normally handled by the webserver as a request for a missing resource and a standard response, resource not found, is sent to the requester. In the experiments the Apache webserver, which offers the web administrator a rule-based rewriting engine for changing requests on the fly, was used [40]. Changing the source code for WordPress or any plug-in was found to be difficult if automation of the process was to be achieved. Instead, we propose to rewrite conditions for when a "not found" response is sent to the requester. Provided a rule condition is fulfilled, we send the request to a purposely-designed booby trap. Once the booby trap is called, the attacker can be offered any desired response without alerting the attacker that something has changed. In our experiment, we were satisfied with logging information. We configured the booby trap to log the requested URLs together with certain request parameters such as the query string and eventual POST data. Stipulate that the objective is to gather complete forensic data about potential intrusion attempts; then the script would be programmed to emulate sought after plug-ins in order to deceive the attacker to believe the attack may have succeeded. Emulation is often necessary since many exploits first attempt to detect whether the actual exploit would succeed or not; the payload itself may not be delivered if the detection fails.

We should note that redirecting requests for missing resources (e.g. files belonging to plug-ins that are not installed) to a special script which handles the requests is not a novel idea itself. Some web frameworks, for example the Yii framework[41] and Fat-Free Framework[42], force requests to go through the main index file of the web application itself if the resource is not found. We employ a similar methodology here, but for a different purpose.

By redirecting bad requests, many types of attacks against a WordPress installation can be avoided. An attack caught by the redirection would not have succeeded in itself (since the requested resource would not have been found), but

[40] For further information on Apache Module mod_rewrite, see https://httpd.apache.org/docs/2.4/mod/mod_rewrite.html. Accessed 30.07.2016.
[41] Yii framework The Fast, Secure and Professional PHP Framework. Accessed 30.07.2016 http://www.yiiframework.com/.
[42] Fat-Free Framework A powerful yet easy-to-use PHP micro-framework designed to help you build dynamic and robust web applications - fast! Accessed 30.07.2016 http://fatfreeframework.com.

we have the opportunity to prevent further attacks, since we can now classify the IP address that made the request as malicious. As an active defence mechanism, this can thus be made a proactive part of the server's security system if e.g. used to automatically reconfigure the server's firewall to block further connection attempts from the implicated IP addresses. This makes the method effective against active scanning by hackers.

5.3.5. Path Randomisation for Resource Installation

To further strengthen the security of a WordPress installation, we also developed a partial method against passive scanning. In passive scanning the attacker cannot be easily detected by normal methods that look for anomalous behaviour, such as requests to missing resources. The previous method focused on missing resources, but offered no added security for installed plug-ins (existing resources). Passive types of attacks may be mitigated by using manual booby trapping, but as earlier stated we found that this is not well suited for the average system administrator nor does it protect against zero-day vulnerabilities. Instead, we explored the possibility of automatically renaming plug-in URIs during installation. Requests using the plug-in's standard URL in a potential exploit would then end up being redirected to the booby trap, using the previously described method. For this approach to be feasible, no manual modification to the plug-ins or WordPress itself can be done. Any manual modification would make their respective update process very cumbersome; the same modifications would have to be re-applied every time a plug-in is updated. Our research shows that this task can be accomplished, at least partially, without editing any existing source code, using something we call *faked redirection*.

Initially we identified three ways in which an attacker may end up running code belonging to a WordPress plugin:

Requests directly to a file belonging to the plug-in

Using hooks defined by the plug-in. The request goes to index.php and is internally routed to a function in the plug-in

Using POST requests to index.php with execution paths similar to those of hooks.

The term *hook* defines a technique used to alter or augment the behaviour of an application by intercepting function calls or messages or events passed between software components. To succeed, all URIs that can lead to plug-in code execution must be rewritten with non-standard names. Requests for the rewritten URLs would then be internally redirected to the original locations, while requests that have not been rewritten would be redirected to the booby trap. This implies that normal site usage is unaffected since all requests go through the modified URLs, but an attacker attempting to leverage an exploit against a plug-in would fail and end up in our booby trap.

The concept may be better illustrated through a simplification with the popular WordPress Download Manager plug-in as an example[43]. Normally, the plug-in resides in "wp-content/plugins/download-manager", and one of the hooks it uses is called "wpdmdl". We now substitute all occurrences of "wp-content/plugins/download-manager" with "wp-content/plugins/faked-download-manager" and all occurrences of "wpdmdl" with "fake-wpdmdl". Here we add, "faked-" to the URIs, but in a real environment this term could be randomised for each separate installation and each plug-in in order to make them unique.

Since we do not want to modify any files belonging to WordPress itself or one of the plug-ins, we use a combination of the *mod_substitute*[44] and *mod_rewrite*[45] Apache modules. *mod_substitute* is used to modify the URLs when the content is served to the browser, while *mod_rewrite* handles the task of reversing the substitution and eventually redirecting requests to the booby trap.

5.3.6. Result Outcome

The aim of section 5.3 was to study and develop new methods for defining and improving the security of the CMS-system Wordpress (cf. RQ2). In an experiment, we set up a booby trapped honeypot server with a publicly available IP and an installation of WordPress. The IP address was not issued a domain name, and therefore not indexed by a Domain Name Server. Hence, each access to the WordPress installation was through the IP address. Because of this, we can assume that any connection either was our own or a potential attacker, automatically scanning potential installations. Our experiments focus on detecting that our booby traps have been activated. Metadata for each attack that is performed against our system and consequently caught by the booby trap, are logged on the server. Manually booby trapping exploits in plug-ins showed some additional limitations, as in cases were the plug-in could be unnecessarily activated through administrative activity. Additionally, booby trapping a plug-in that is included on the main page (index.php) is not recommended, as all site traffic should then be filtered.

On the other hand, redirecting requests for missing resources was quite successful and many potentially malicious requests were logged. This includes those aimed at exploiting software other than WordPress. Our technique also detected attempts to discover vulnerable versions of WordPress plug-ins, which were not installed on the server.

---

[43] For the source code to WP Download Manager, see https://wordpress.org/plugins/download-manager/developers/. Accessed 30.07.2016.
[44] For the specification for mod_substitute, see https://httpd.apache.org/docs/2.4/mod/mod_substitute.html. Accessed 30.07.2016.
[45] For the specification for mod_rewrite, see https://httpd.apache.org/docs/2.4/mod/mod_rewrite.html. Accessed 30.07.2016.

Initial testing shows that the path randomisation method has the potential to catch malicious requests. The faked redirection technique for installed plug-ins detected connections that were attempts at exploiting vulnerabilities. Without the faked redirection technique in place, the above requests would have succeeded since they are perfectly valid. Further study should be performed as to determine if the technique could also catch zero-day exploit attacks. However, a zero-day exploit tends to have a monetary value, and the use of these exploits tend therefore be limited to situations where the attacker can gain a monetary return. Each time the attacker uses a zero-day exploit to attack a system it poses the risk of becoming known and eventually fixed/unusable.

The focus of our study was on mitigating effects of automated scripting attacks. For the most ardent of attackers, the path randomisation method may be less successful if the attacker manages to find the randomised paths, e.g. by guessing or through references. The proposed method should be studied further to determine potential weaknesses. However, in combination the three methods presented offer the system administrator a path towards active defence against malicious attacks (cf. RQ2 and RQ2.1). Combining these methods should be particularly useful against fully automated attacks, where the attacker is not targeting a specific system, but rather scans the Internet for any potential target. Furthermore, our methods offer machine learning based network intrusion detection a novel way to create labelled training data. This offers the opportunity of further exploration in the use of big data in network intrusion detection, defence, and forensics.

Our goal is not to build a platform; it's to be across all of them.

—Mark Zuckerberg

6. Platform privacy

The previous chapters have primarily analysed the ambiguity of the GDPR from a technical and service design point of view. However, in recent years we have witnessed a shift of focus from individual services/products to platforms and ecosystems of users. The Regulation has largely addressed the service side, but while the debate regarding its existence has been dragged out over the last 5-10 years, Internet technology (software) has gone through an evolution of several generations. In consequence, business models have shifted form as well.

The transfer from a digital product to a service is to a large extent technology driven. We can determine a fundamental difference between product and service in how both user data and application data are stored. In the product, data are often stored locally (on the device), while in the service, data are stored on a server or in "the cloud". Going from a service to a platform is however a more strategic decision (Gawer and Cusumano 2008). Building a platform means striving to create a two-sided market. The focus then becomes one of enabling other service providers to join the platform and matching them to consumers/customers of said platform, while the platform owner levies a transactional fee on said interaction. The exchange medium in the loop between service producer and consumer was defined by Parker et al. (2016, p36) to be either information, service, or currency. The more positive feedback loops that can be built into the platform, the stronger the platform tends to get. The platform can then be described as an infrastructure for facilitating the exchange loop(s).

A right to personal data portability and data security both have an implication for the platform, but in the Regulation both are mostly limited to an elementary impact. However, in today's information system environment, platforms are considered an integral part of a successful launching of a scalable service. We can argue that the new Data Protection Regulation was already too extensive to include a more thorough deliberation on platform issues. Consequently, in September 2015 the EU Commission launched a public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy (European Commission 2015). The consultation focused on gaining a better understanding of online platforms and the need for further regulation. In particular, the consultation focuses on illegal content on platforms, such as copyright issues, but it also highlights transparency issues. Here we continue with a focus on the privacy rights issues that are closely linked to data protection, which we find is not sufficiently elaborated on in the GDPR (cf. RQ3). In this chapter, we will argue that regulating privacy and personal online security from a platform point of view offers the best opportunity to achieve a more trusting relationship between those that provide services on a platform and their users.

Platform owners have so far had very little incentive to develop platform privacy and the relationship to the platform users (both producers and consumers) are mostly governed by unilateral contracts, i.e. provider defined.

6.1. Platform challenges with the GDPR and current practices

This section analyses the GDPR from two different positions to better understand issues that arise from the extensive use of digital platforms. The first perspective is data protection for the individual and the second aspect is improving conditions for competitiveness for new digitalisation business ventures (including both incumbent institutions and start-ups) in relation to the already dominant Internet companies. The latter position is thus an analysis of how the Regulation could increase competition in the market, as a guarantee for better privacy. Section 2.8 reviewed the literature for the theory on platform economy, here we continue by connecting the theory to the design and practice of such platforms. To achieve this, we will first briefly review the current literature on digital platforms and then analyse how the Regulation deals with current practices that are linked to the platform.

Many of today's successful digital ventures are considered to take the form of a digital ecosystem where companies and consumers coexist. The Android mobile operating system is often used as an example of such an advanced ecosystem. A digital ecosystem is often described in terms of its natural counterpart, where adaptivity, competition and sustainability define the success of the ecosystem. Lyytinen and Yoo (2002) started the analysis of such environments based on their identified trends in technology of mobility, digital convergence, and mass scale. Research from an economic perspective has verified that the ecosystem often can be described as a platform for multi-sided markets (Rochet and Tirole 2003). When Gawer and Cusumano (2008) argued that creating either a platform or service is a strategic decision, they considered a service to be an early version of a platform, a service that can also exist upon another platform. For a service to become a platform, they considered that the service must satisfy two prerequisite conditions: performing at least one essential function that can be described as a "system of use" and secondly the system should be easy to connect to or to build upon to expand the system of use.

From a technological perspective we see that scalable information system architectures are today often designed on the principle of microservices (Dragoni et al. 2016). A microservice is a specialised self-contained software system that communicates through lightweight mechanisms and with a bare minimum of centralised management of these services. The services may be designed in different software environments and use different data storage technologies, but communicate through a well-defined application programming interface (API)

while using a generic protocol. This type of architecture is particularly well suited for building digital platforms that are highly efficient and allow for user data to be moved rapidly between services for processing. The technical distinction between service and platform is disappearing when the service is designed as a microservice. A microservice architecture can be seen as a distributed enabler to achieve service scaling in the cloud computing environment. The microservice can contain any needed business logic for its independent existence and communication with others. From a technical perspective the platform is often defined as the communication medium. This communication medium can take many business forms, for example as a market for distributing games and applications between consumers and third parties. An important insight from Henfridsson and Bygstad's (2013) work on generative mechanisms is the role adaption plays in the availability of user data. The availability of extensive user data that can be cross-referenced with similar data from other users is at the core of the success of a digital platform.

In a Gartner report, Ekholm and Blau (2014) analyse the next step in the evolution of the personal cloud connected to the vision of Internet of Things. They use the term Cognizant Computing to describe how analytics can be used "*in order to increase personal and commercial information about a consumer through four stages: "Sync Me," "See Me," "Know Me" and "Be Me"*". A closely related field with a consumer perspective is virtual personal assistants, which by observing its user's behaviour, builds and maintains data models, with which it draws inferences about people, content, and contexts. Austin et al. (2014) define the virtual personal assistant's intention as "*to predict its user's behaviour and needs, build trust and, eventually, with permission, act autonomously on its user's behalf*". They estimate that current dominant companies such as Apple, Facebook, Google and Microsoft will be best positioned to embark into the new era, partly because of their already existing access to massive user datasets. The vision set forth states that, in order to benefit from them, it will be in the data subject's best interest to open up as much as possible of our life to the companies that offer these services.

In their work Henfridsson and Bygstad (2013) present the view that previous research into digital infrastructures fail to articulate "*the multiple paths by which successful digital infrastructure evolution comes about*". They pose the argument that "*there is a tendency to offer partial explanations, rather than focusing attention on the complete set of key mechanisms and their interaction.*" The question we raise based on the discussion of past, present and future is whether this is true of the rational governing the legal texts as well. Instead of examining data protection through modularity (cf. articles in the Regulation) or individual forces that exert pressure, we ought to examine this from a more holistic perspective as a function of a service objective (cf. RQ3). How can a Data Protection Regulation return and retain the individual user´s trust in digital services, while maintaining the generative

mechanisms needed to build tomorrow's platforms that employs intelligent services?

After examining the Regulation we find that the core aim seem to have been just that, to create a Regulation that form the basis for a unified view. The secondary aim, at least considering the final version, is still not focused on the generative mechanisms and will e.g. not force the platforms to open up their data silos. Zittrain (2006, p.2027) considered that to achieve generativity, systems must be open and adaptive. Arguably, the Regulation consider instead that the use of data is minimised and preferably anonymised, and thereby unlikable to the data subject. As Henfridsson and Bygstad (2013) also found typical in their research, a partial explanation is offered by the Regulation by this static view of data, still we can consider that most platforms and intelligent offerings strive for an opposite explanation.

One can make the argument that the Regulation should not deal with platform issues or intelligent offerings, but rather focus on the data subject and his personal data. The Regulation has already grown about 10 times compared to the Directive and has become a relatively complex piece of legislation. The EU Commission strategy for a digital single market identifies the open questions of platform regulation to determine the regulatory environment for platforms, online intermediaries, data, and cloud computing, and the collaborative economy (European Commission 2015). Here we will continue examining the privacy rights issues for platforms that are closely linked to data protection, which we find is not elaborated in the current Data Protection Regulation. In the following sub-sections, we will focus on platform issues that are not taken up or addressed sufficiently in the Regulation, but that may improve the trust and generativity in platforms and intelligent services.

6.1.1. Managing Consent for Services on a Platform

As categorised in sub-section 3.2.4, the Regulation defines lawfulness of processing so that each interaction between the data subject and the controller involving personal data identifying the subject, starts with the data subject consenting or contracting to the processing of this data (GDPR 2016, art. 6(1)). As described later, common current practices particularly in regards to contracting, often strive to outmanoeuvre or simply void the purpose of earlier described legislation. Maintaining a limited number of these often highly complex contracts and/or consents ought to some degree be possible for the data subject, for example email, search, operating system/platform, and social network. However, exceeding a certain number of these consents and contracts will make it implausible for the average data subject to remember what he has agreed to and with whom. Currently each application installed on a smartphone or service on the Internet is required to maintain their separate contracts when handling personal data. With the present

system, it will over time likely become unmanageable for the individual to control his digital presence when sharing personal data. For the data subject it will be virtually impossible to obtain an overall picture of collected and stored data, which in turn leads to difficulties in making decisions about deleting specific data. In our view the established legal practices sets unreasonable expectations on the data subject. A more appropriate solution would be to impose an obligation on the platform controller to periodically submit or on request provide information to the subject regarding what data have been collected for any platform service, how data have been processed, the results of the processing, and to whom the data have been shared (cf. RQ3). The GDPR states that a controller cannot defer any legal undertakings to a third party, as the ultimate responsibility remains with the original collector of consent. As an example, a mobile platform controller is the collector of the original data subject consent to use a platform which involves the processing of personal data. The platform controller should thus be given an additional obligation that includes the management, storing and maintaining of specific consents to any additional third party services (i.e. applications or games) distributed in relation to the platform. Today most mobile platforms only register the permission details granted to applications that give them access to certain platform APIs, for instance a location API to access the geo-location of the user. Currently it is often impossible for a data subject to retrieve any information from the platform concerning when a service accesses personal data and processes or distributes it further. The said service would still need to collect a specific consent from the data subject, but would also be obliged to submit information back through the platform on processing details. This would allow the data subject to more easily gain a transparent overview on how data are collected and used in extension of the platform. Accordingly, a platform controller should not be allowed to defer responsibility for any processing that occurs by the means of a service provider in relation to said platform. The platform controller provides the means for the service offering and benefits from any monetary transaction on the platform, thus the legal framework ought to define the platform controller's obligations so that a transparent view of processing by a service provider can be easily obtained by the data subject.

The Regulation delegates a similarly unreasonable expectation upon supervisory authorities. Their duties include e.g. launching investigations on their own accord and certifying controllers and processors as to let data subjects quickly assess the level of data protection provided by any service provider. We consider the proposed certification mechanism to be a plausible idea for improving trust and transparency, but the implementation and collection of compliance records is questionable. The supervisory authorities of the Member States will not have resources to perform this task adequately, as it is now defined. Certifying a platform, e.g. a mobile operating system, will require in-depth technical and considerable monetary resources to perform the certification with any credibility. For a company to merely state

compliance to some defined notion of privacy, without there being any transparency in regards to processing in said platform or service, does not initiate trust on a general level (cf. RQ3). As a solution to the issues of certifying services on a platform, a similar solution as described in the previous paragraph would offer supervisory authorities means to more easily identify data protection issues that may arise from unlawful processing. Provided a supervisory authority is granted access to random checks of said platform/service data, for the purpose of verifying that said service abide by the consent contract and the law, a certification would signal some level of trust.

6.1.2. Discriminative practices against privacy-aware users

The business world is facing a challenge in adopting new technology to process big data (high-volume, high-velocity and/or high-variety data) and establishing new revenue models based on big data analysis. The balancing of user privacy is equally demanding, particularly when the availability of data is linked to the future success of the platform. This creates a difficult balancing act where data protection may be on the one side and the company's future prosperity is on the other. The definition of personal data in the Regulation limits its applicability to physically identifiable data subjects, thus there is a lack of protection for virtual identities. An example given in sub-section 4.2.6 was an online forum that tracks users without asking for or storing any information referring to the identification of a natural person. The example illustrated how it is possible for a service provider to profile users without the possibility to identify the physical identity of the user.

In comparison, data that have undergone pseudonymisation, which could only be attributed to a natural person by the use of additional information from a separate data source, should be considered as information on an identifiable natural person. A similar protection does accordingly not apply to virtual identities. Although, the natural person's physical identity can be irrelevant for profiling with the intention of e.g. direct marketing purposes, the protection for virtual identities hence fall outside the scope of the Regulation, as the Regulation only applies to data concerning an identified or identifiable natural person (cf. RQ1 and RQ3). This may have an implication for decentralised blockchain platforms as well, as the user's identity is normally not revealed. A controller of a blockchain service may thus process data relatively freely, provided attempts are not made to identify the physical user by storing any such data that can link to a natural person.

We continue this sub-section by examining some current industry practices that we find challenging for the Regulation. We find these practices to have a detrimental effect on the individual's ability to choose his or her level of privacy and data protection. Declining giving the controller rights to user data for these services will effectively mean a refusal of service by the controller.

6.1.2.1. The right to use pseudonyms

Common practice in the design of current platforms, e.g. smartphone operating systems, is to require the user to identify themselves through a physical identification mechanism in order for the consumer to be able to make full use of the platform and its services. This can e.g. take the form of linking a phone subscription (number) to the profile of the smartphone platform operator, by requiring the consumer to enter a code sent by SMS to the phone. Employing a mechanism that requires physical identification suggests that all platform operations and services distributed on said platform are legally bound by the Regulation. Hence, e.g. each application consequently installed on a smartphone should ask for the data subject's permission to store and process data. A similar authentication process is also often used for signing up to a web service. The question we want to raise is whether the platform owner should be allowed to require a physical identification mechanism such as linking an email account to a phone number or a credit card, unless there exists an explicit legal need for identification. As defined earlier, the controller has a monetary interest in collecting data by means of user profiles. Being able to combine data from the physical world with the digital makes the data collected easily transferable as a service to other companies and thus a tradable instrument. However, there can also be certain service quality reasons for employing methods based on verified physical identities. For example, it can be argued that using a real identity makes users more aware of privacy. Due to the user having to make a conscious decision in the linking process, the user is also likely to be more vigilant in what information is shared in the future. Another argument is that the use of "real names" helps in keeping the community safer, by reducing malicious activity and in improving methods for detecting such activity.

Nevertheless, the data subject's inability to make a conscious decision whether or not to link the physical identity to said user profile should not be considered best practise. For example, in the case of smartphones, linking a pseudonym (or virtual identity) to a hardware-based device ID should be considered adequate, without the consumer having to identify himself by physical means. This refers to the process of logging in with credentials governed by the smartphone OS operator to make use of said device. In the case of public safety reasons, authorities have other means to cross-reference a device ID with a natural person through the telecom operators. The issue of pseudonym identities has also been raised by German regulators in suggested amendments to the current proposal as well as in its interpretation of current German data protection law (Unabhängiges 2015).

6.1.2.2. Privacy policy as a lock-in mechanism

Privacy policies (or data policy or terms of service) governing the digital relationship between the controller and the data subject are often complicated matters. Research has shown that more than half (52%) of Americans do not understand the purpose of a privacy policy (Smith 2014). Through a longitudinal study they observed that there has been little progress in awareness during the last decade. The majority of respondents still believe that the intention of a privacy policy is that the controller agrees to keep user data confidential. Facebook (the social network service) has perhaps one of the most publicly discussed terms. Facebook's policy states that the user grants Facebook "*a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content*" [46] that is uploaded. The company also reserves the right to transfer the users' information between their other services such as Facebook Payments, Instagram, and WhatsApp in accordance with their respective terms. Thus, a situation is created where users become so intertwined and dependent on said company that they arguably can be considered locked in. Harrison et al. (2015) found four broad categories of service relationship lock-in factors: "*Moral/Obligatory Factors*", "*Personality Factors*", "*Switching Costs and Lack of Alternatives*", and "*Positive Benefits of Staying*". These factors all contribute to creating the privacy paradox. At present there are very few other options for a digital social network than Facebook. However, Facebook has become more than a social network. Today we can consider them '*The global communication platform company*', often superseding traditional telecom carriers in voice, text, video, images, and directory services. This is in addition to their original and still core service of users receiving notifications when friends update their profiles.

The issue we aspire to highlight with this discussion (cf. RQ3) is that from studies regarding network externalities we know that digital service companies that can manage to lock-in their user base, tend to be able to create and sustain a "processing silo" within certain segments (Haucap and Heimeshoff 2014; Argenton and Prüfer 2012). There are arguably other social network companies than Facebook, such as Twitter, but they are currently competing within different segments of the market. [47] Even Google, who tried creating a competitor to both Facebook and LinkedIn, Google+, has not succeeded in getting users to switch and start using the service. In the Google+ case it is worth mentioning that Google started with a massive persistently signed-in user base from both its email service as well as Android operating system. These users were then often reminded that they could merely turn on the features for Google+ by clicking an acceptance link. Haucap and Heimeshoff

[46] Facebook Terms of Service as of 30.1.2015, Accessed 22.09.2017, https://www.facebook.com/terms.

[47] Facebook is estimated, by Statistica 2017, to have 2.05bn global users, whereas the total number of social network users worldwide is estimated to be 2.46bn. Accessed 22.09.2017, http://www.statista.com/topics/1164/social-networks.

(2014) reasoned that if a company can create a proprietary single platform, then strong network effects can lead to a highly concentrated market structure. In contrast to traditional wisdom regarding monopolies, strong network effects in digital services also tend to make highly concentrated market structures efficient. Haucap and Heimeshoff (2014), find that this efficiency leads to an unambiguity in how market concentration affects consumer welfare.

Spulberg and Yoo (2014) argued that the network effects are not a source of market failure in their denouncement of heightened antitrust scrutiny of network industries. They observed that vertical integration and vertical restraints tend to promote, rather than harm, competition in network industries. The above example of Facebook tends to suggest the same; vertical integration in the company has led to what we consider a disruption in the whole communication sector globally. What Spulberg and Yoo (2014) seem to fail to recognise in their analysis of natural monopolies within the Internet sector is that initial competition within an emerging segment does not equal continued competition, given that "processing silos" are created and maintained. The lock-in factor at play in today's platforms mostly relate to access to user data [48] and not infrastructure (cost inefficiencies), service innovation, or price regulation as they suggest. In the Google+ case this was quite evident; the service itself was considered good by many, including media journalists (Duffy 2012). However, when it came to user contributed content, very little existed. Those that tried out Google+ often did not want to keep cross-posting status updates. As a consequence, the uptake was lacklustre and critical mass was not achieved.

Many of the EU Member States have good earlier experiences from the regulation of platforms. The telecommunication sector has been transformed through regulation from local regional carriers to a functioning pan-European service market, with some of the lowest prices and highest quality services in the world. The original GSM mobile communication network that was allotted to two or more operators, were divided by Member State and not region. The Member States bound the interested telecommunication operators to adopt the 2nd Generation GSM standard through a competitive tender (Eliassen et al. 2013). The change introduced the consumer to a choice of network operator, which could for the first time be based on personal preferences. Eventually, in some countries, e.g. Finland, even allowing the consumer the option to transfer the phone number between operators. This option was important, because it removed the last lock-in mechanism available to operators, to "force" consumers to stay with them (cf. RQ3). This indicates the regulator's power to change market dynamics on its own accord for the benefit of the consumer. The regulatory environment improved conditions for European companies by increasing the market size, but also created an enriched roaming

[48] We define user data to include describing, behavioural, created and generated data.

experience for European citizens. Comparing to the social networks of today, the alternative to a non-regulated mobile telecommunication infrastructure in Europe would have been that each operator had developed their own technology that would have been incompatible with that of all other operators, including communicating from one network to the other. This would likely have created an ecosystem with a few pan-European or worldwide operators that most likely would also have manufactured their own equipment. From a business point of view this had not perhaps been a failure of markets, but from a consumer point of view a drastically inferior experience.

6.2 Exemplification of the importance of platform privacy when integrating future Internet of Things enabled services

This chapter has examined present practices and relevant legislation in connection to platforms and privacy. In the following example, we want to illustrate what can be expected from the digital services of tomorrow. The intention is to imagine a technological vision, serving as a guidance and motivation for the discussion in chapter 7 on a proposal for both an architectural change (cf. RQ2 & RQ2.1) and a different legislative environment for platforms (cf. RQ3).

During recent years we have seen the introduction of the first Internet of Things-enabled devices for the consumer market. Among the first such products launched were personal health-monitoring devices. These were first exclusive for various fitness enthusiasts, but have later on been introduced as mass-market products. These types of products can continually monitor a user's activity, location and certain bodily functions, such as heart rate, brain activity, or glucose. An example of an advanced intended use case is to be able to remotely monitor individuals, such as elderly people in their own homes. The intention is to enable the individual to continue living at home as long as possible, while alerting relatives or health supervisors if an anomalous event occurs, such as the person falls down or becomes ill. In addition to personal health measuring devices, sensors measuring impact are being built into floors, motion detection is used for measuring activity, energy use is measured to prevent appliances from running amok, audio recognition can be used for detecting shouts for help, to mention a few. Essentially, the more complete and real-time data we have about an individual, the better the service quality can be made. In addition to previously mentioned data types, we are here referring also to behaviour, usage, the individual's social network and their corresponding data. The example illustrates how sensitive the information gathered can be and to what the technological progress is heading. Data flow for this type of service often includes limited storage on the sensor device and with long term storage in the cloud. Often there is an intermediary device required as well, e.g. a computer or a smartphone, were data is cached within a certain application. User data is hopefully always secure

and encrypted but this is not possible to explore for an average user. The processing of data would likely be in the cloud, provided the data communication is real-time.

The example highlights the positive application and progressive use of data collection and processing for the purpose of creating intelligent prescriptive services (cf. RQ3). However, from a legal standpoint the intention of the Regulation is that data should be collected, processed and stored in a data minimising way. At the same time, the Regulation does not provide the data subject with the right to review the security in the data flow for the platform/service. As data subjects we are currently forced to trust that the controller collects data in a minimalistic way, processes data only with the data subject's best in mind, stores data securely, always promptly notifies us when data are shared or breached and, given that the subject wants to close the account, taking for granted that the provider actually deletes all data in a non-retrievable fashion. This is the primary reason we consider the rationale behind the Regulation to be antiquated and why we call for an increased focus on platform privacy. Closed systems tend to instil distrust as a lack of transparency into said systems means any processing or security can and should be questioned in terms of validity.

The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom.

—Isaac Asimov

7. Discussion and Future Research

Trust as a key design goal for information systems encompasses a wider definition than data protection in the Regulation. Trust includes, inter alia, security implications such as an ability to easily switch between different platforms and choose between different service levels. This thesis presents an understanding of trust that also includes processing on data which is generated by man or machine alike, without any direct separation of data linking to a natural or virtual person. The example provided in section 2.4 of Microsoft's experiment with a chatbot that learns from previous communication showed that increasingly, through a symbiotic process, algorithms and humans will develop a collective intelligence (Malone and Bernstein 2015). Recent claims against Google's search engine suggest that a similar symbiotic learning process has revealed sensitive information regarding for example the identity of juvenile delinquents, where the search algorithms have learned and extrapolated from other users' interaction (Duffy 2017). Although such symbiotic relationships are the aim of many intelligent personal agents, they are likely to cause clashes with the legal view of data protection and privacy in general. Trust as a key design goal is further discussed from an intelligent system design point of view in section 7.1, from a technical viewpoint in section 7.2, and from a platform viewpoint in section 7.3.

Data protection as a term in the EU legislation is reserved for defining the lawfulness of processing personal data, whereas, the term privacy is not used in the Regulation. Privacy on the other hand can be considered to be used in the US as an extended synonym for data protection. Examples of such US laws that define sectorial privacy are the Health Insurance Portability and Accountability Act[49] and the Children's Online Privacy Protection Act[50]. Both terms used in their respective setting tend to be limited in regards to security aspects of how to keep data subjects safe. Security can be defined through a number of viewpoints in digital services, e.g. information security, network security, access control, or availability. Section 7.1 highlights some important interpretations that can be derived from the GDPR, particularly in regards to such processing of personal data that leads to profiling and automated processing. The ambiguities in the GDPR discussed in section 7.1 present an architectural design such as client-side processing as a way of avoiding many of the issues that personal data processing services encounter with a traditional centralised architecture.

[49] Health Insurance Portability and Accountability Act (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996).
[50] Children's Online Privacy Protection Act (COPPA; Pub.L. 105–277, 112 Stat. 2681-728, enacted October 21, 1998)

An EU Directive on Network and Information Security (2016/1148) was adopted to, inter alia, establish security and notification requirements for operators of essential services and certain digital service providers (NIS, art. 14(3) and art. 16(3)). The operators are to be identified by Member States continuously, on criteria related to defining an essential/critical service in the Member State, including digital infrastructure of non-traditional Internet industries. However, such Member State lists are not considered complete or limiting, rather companies should be vigilant in determining their own stature within the various Member States. NIS can be considered providing an operator with a minimum level of obligations related to their information systems security. It should be noted that the NIS is not legally applicable for a great deal of digital platform and service companies. Rather the NIS can be considered a minimum best practice for these companies. All companies processing personal data are guided by the GDPR, and are thus required to use appropriate security to reduce the risk and scope of security incidents. The term appropriate security is discussed and a proposal for what should constitute appropriate security in a modern information system is provided in section 7.2.

One of the GDPR challenges identified in the thesis is how to handle personal data in connection to platforms. We have presented the concept of the platform as a processing silo that from a legal point resembles the discussion in the 1990's surrounding telecom operators and their ability to lock-in customers. We have highlighted that a marked difference between then and now is how the cost for using the service is determined, highlighting the issues that arise from the consideration that the interchange of personal data means that no monetary payment has been provided. Thus, today many platform operators consider the data subject a 'user' and not a 'consumer', with the corresponding rights that have been established over many decades. Changing this dynamic will be difficult, as currently the vertical integration among the more successful platform companies, have led to that few other alternatives may exist. The efficiency in using the network effect has enabled the platform companies to develop a business model that in many other consumer-facing industries would be considered either monopolistic or oligopolistic. In section 7.3, we highlight three problem areas that need to be addressed by a future EU Regulator, provided that these platforms as maintainers of processing silos are considered problematic. Here we limit the focus to the GDPR, but this has a much broader implication for the Regulator, for example by involving policies on anti-trust, consumer protection, national security, and taxation.

7.1. Design of Intelligent Systems Handling Personal Data

Processing that aims at creating data subject profiles or automated decision making which creates a legal effect or significantly affects said person, is limited to situations where consent is given or for the performance (or in anticipation) of a contract. Additional provisions apply for such processing as the data subject can demand that

the controller provides human intervention and that any decision is contestable (see chapter 4 for further analysis). The full implication for intelligent systems will only become known over the coming decades when these services are rolled out and the courts further define the implication. There has been discussion in the EU Parliament of regulating AI and robotics further that, at the time of writing, has led to a report with general considerations for what aspects can and should be considered if constructing regulation (European Parliament 2017). The subject of how to govern AI and AI-enabled robots including the accountability aspects of AI algorithms, although interesting for future research, is outside the scope of this thesis. Here we focus on the privacy aspect of intelligent services and pose the following research question:

RQ 1. What are relevant interpretations and ambiguities for information systems that can be derived from the GDPR, particularly in regard to such processing of personal data that leads to profiling and automated processing?

The symbiotic learning relationship between man and machine is likely to continue to interest researchers for decades ahead. Let us here consider the issue from the perspective of designing trusted personal assistant agents that conform to the privacy rights in the EU. We can find a connection to information systems research in how these agents are trained and how training data are sampled. In both Microsoft's and Google's case the algorithms are trained using normative (group) sampling, and this can also be considered the most common approach in current use. This means that the training sample is based on the interaction of all users. Thus, something learned from one user is generalised and transferred to any other user. We can define *normative learning* as that the subject acts rationally and that analysis of the group provides insight into the individual (cf. section 2.1) (Lorscheid and Troitzsch 2009; Tuyls and Parsons 2007). A different approach to the problem is to focus on learning using individual sampling, thus *descriptive learning* assumes that the subject is irrational and requires analysis of the individual subject in order to gain insights into his behaviour (Tuyls and Parsons 2007). Normative learning in contrast aims to introduce prescriptive elements (e.g. opinions of other users) that may offend and/or propose moral values that are not generalisable. This separation of sampling may offer researchers/developers an approach toward creating agents that are compliant with the European fundamental rights. To use an analogy, each citizen can claim a right to freedom of expression provided no harm or offense is incurred on any other natural or legal person. Individual sampling can be likened to the right to freedom of expression while normative sampling can at times introduce harming or offensive behaviour into the agent. When the symbiotic relationship is exclusive between the agent and the human, we can consider any potential offensive behaviour self-induced. Thus adopting trust as a key design goal for agents suggests that individual sampling for descriptive learning offers a path forward that is guaranteed to be compliant with the GDPR. For normative learning to be compliant, a generalisation criterion must be defined for the transfer learning between individuals to occur. The criterion should take into consideration the possibility of the training sample containing a learning bias that may be offensive.

To design prescriptive services, one needs to go beyond data minimisation as required by the GDPR (cf. section 2.8). To ensure a high decision quality of digital personal agents using prescriptive techniques, it will require that the data subject provides the algorithm with every single data point that refers to the data subject. The more comprehensive data that exist as input for the model, the better the output result can become. However, we can consider it likely that data from the

surroundings will improve the model further. Techniques for obfuscating data are a current and important research topic, for example differential privacy considers how to add (mathematical) noise to data in order to improve the privacy of data collection practices. A different type of method that is being researched is the use of distributed ledgers (e.g. the blockchain) for storing personal data (Mainelli 2017). The distributed ledgers would add cryptographic security, access control, access logs for forensic investigations, and perhaps most importantly would remove the central point of failure. A company without complete access to the data subject's data will be unlikely to launch a successful intelligent personal assistant service that utilises prescriptive analytics to deliver decision support or acts on the behalf of the data subject. Gartner's prediction that current platform companies will be the ones leading this new area is thus very likely (Austin et al. 2014). Platform companies with a high degree of vertical services on the platform will be best positioned to legally collect data in a broad sense that can then be utilised in the creation of tomorrow's intelligent services.

An ambiguity identified in the GDPR is how client-side processing that occurs outside the direct control of a controller should be handled. Recent launches of smartphones have specific hardware included for enabling efficient operation of machine learning algorithms. Client-side processing has been possible in the browser on desktops, but the introduction of new hardware in smartphones creates new possibilities for building intelligent services for mobile devices that do not need to communicate with a centralised server to reach a decision. This probes the question that, provided no communication using personal data with the outside world is implemented in said service or application, how does the GDPR then apply to the design of intelligent services. As in the example presented (section 4.2.6) with virtual identities that do not receive protection, we can only assume that the application of the GDPR would be limited, for example, in the case of client-side profiling. As the applicability of the GDPR is connected to the ability of the controller, or third party, to directly or indirectly identify a data subject using personal data, then in such cases where client-side processing offers no ability for the controller to access such data, we need to consider whether the GDPR is applicable or not. These are the types of boundary cases that will likely require further elaboration by the courts. As an observation, from a data protection point of view one can make the argument that client-side processing would in many cases be preferable to server-side processing, because of data minimisation and privacy by design requirements in the Regulation. However, in the longer perspective we may need to verify that the algorithms are dependable and accountable, and this may require additional legislation that has an implication on how autonomous agents operate and report.

An interesting aspect for information systems researchers is how management support systems will be affected by the GDPR when processing personal data.

Considering in particular the lawfulness of the analytical component of MSS and similar consumer facing systems provides information systems researchers with a new and highly relevant field to research. The GDPR does not make any distinction between personal data when it is handled for employment or for health reasons, compared to for instance direct marketing. The thesis has connected MSS to the GDPR by considering the level of automatisation in expert systems (fully) and decision support systems (partially) respectively. Automated agents acting on the behalf of the data subject has also been introduced as a concept for describing digital personal agents, albeit these are still in their infancy. The use of fully automated expert systems will thus likely be limited to processing that does not use personal data. Decision support systems that handle personal data must support manual intervention at every decision making step in the process.

7.2. Active Network Security in Scalable System Architectures

The GDPR does not define measures for system security, but states that appropriate security must be used. This section provides a discussion of findings in the thesis concerning what should constitute appropriate security. We highlight through three exploratory case studies (cf. chapter 5) the need for adaptive security and the integration of data generators built into the software, in what we define as *active network security*. The network term is inserted to capture that in virtual environments nearly all the threats materialise over a network connection, hence active network security is not only concerned with the transportation layer, but also includes suspicious use of or direct attacks on end-points, such as API's and web user interfaces.

In Grahn et al. (2017) we define a taxonomy for active network security that considers near real-time techniques for improving network security. Figure 5 illustrates the taxonomy categories from the perspective of an analytics workflow. It should be noted that active network security extends beyond adaptive network security using analytics into, for example, booby trapping and the identification and application of advanced security measures to be taken after an intrusion attempt/event. In addition, active network security should be seen as complementary to passive methods, and not as a replacement.

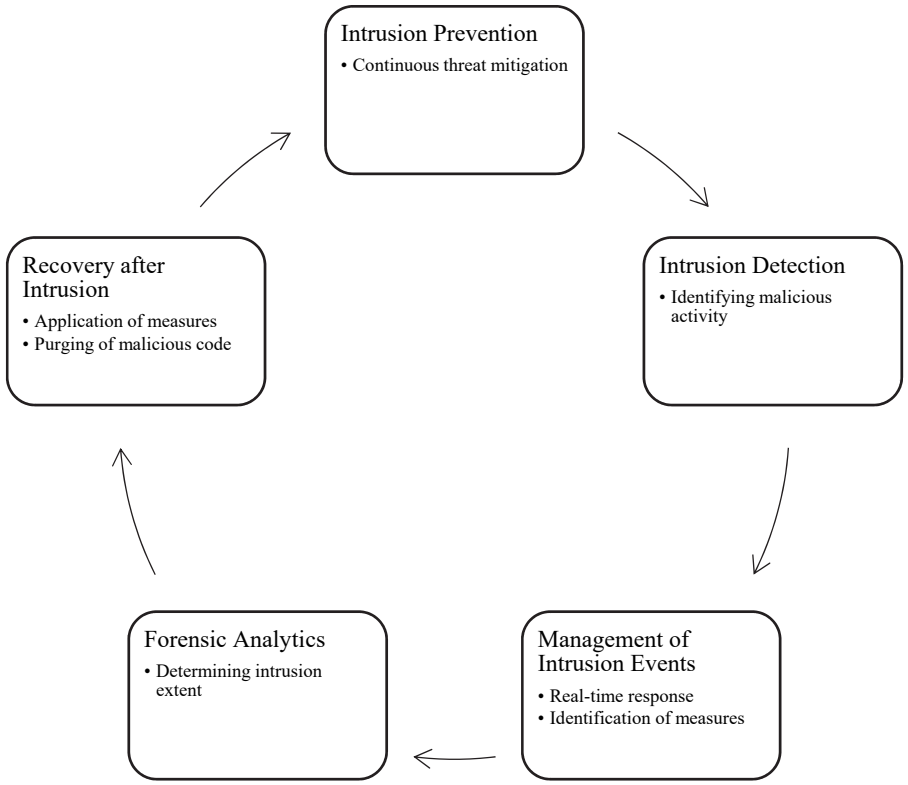


Figure 5 - Active network security taxonomy (adapted from Grahn et al. 2017)

The discussion in this section attempts to answer the following two research questions:

RQ 2. What future technical implications can "appropriate security", defined as a legal requirement for lawful processing under GDPR, entail for scalable information system architectures?

RQ 2.1. With focus on security in publicly accessible software, what is a viable technology basis for a scalable processing architecture?

The combination of scalable systems that can potentially handle billions of users and traditional passive security is problematic because of the impact on society when a breach occurs (Newman 2017a, 2017b). Once an attacker gains access to such a system, it may mean that the complete data store can be accessed and transferred outside the company network without the controller's knowledge, as in the Yahoo case (O'Brien 2017). Any software installation accessible over the Internet is potentially vulnerable, and thus such systems should always be designed and built so that even if an attacker gains access, the potential for damage is limited to a small number of users. This requires that the attack can be detected in near real-time and

that detection and decision-making is automated. The attack vector may differ depending on whether the software is proprietary or open source, but both source types are similarly vulnerable if the software is not kept updated. [51] [52] So-called one-day attacks occur when a bug is publicly known but not patched, whereas a zero-day attack occurs when a bug is known by the attacker but not by the public. By definition the system owner can defend against one-day attacks by either updating the software or by taking the software offline when a bug is identified, while zero-day attacks typically are very difficult to defend against. In section 5.3 we present the preliminary work on a novel method for defending against both one-day and zero-day attacks on web software. The aim of our work was to develop a method (a set of techniques) that improve the ability to defend against both one-day and zero-day attacks, which can be applied to an installation without any significant changes to the existing codebase, and to enable active security management by implementing data generators that can be connected to various analytics-based security systems. In section 5.2, we provide a study of such an analytics-based security system for network intrusion detection. The method for defending against both one-day and zero-day attacks on web software is based on three techniques: booby trapping, redirecting requests, and path randomisation. Although the difficulty in showing conclusive proof of its effectiveness against any possible attacks today or in the future, preliminary findings are positive. Future research could be conducted as a longitudinal study of how well the system withstands attacks by setting up a honeypot server and connecting an analytical security management solution for detecting anomalies and controlling traffic. By continuously monitoring new bugs and their consequent patches for a longer time, we would be able to monitor the different attack vectors used and how well our method withstands the test of time. Section 5.1 provides an insight into the low-level architecture of scalable systems underlying so-called Analytics as a Service (AaaS). Based on these three explorative studies in chapter 5, the thesis highlights the converging trend towards distributed architectures, adaptive security based on analytical methods, and the use of data generators inserted into public end-point installations.

7.2.1. Distributed Architectures and Decentralised Systems

The traditional information system architecture usually aims at separating the application logic (i.e. the implementation of the business logic) and the data store. Connecting the application logic and the data store with an enterprise service bus

[51] An example of an attack on proprietary software, https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

[52] An example of an attack on open source web software, https://qz.com/1073221/the-hackers-who-broke-into-equifax-exploited-a-nine-year-old-security-flaw/

became the foundation for the centralised monolith architecture. However, in practice the enterprise service bus often also connects different application logic modules together, thereby contributing to the difficulty of detecting intrusions and massive data leaks by monitoring the traffic on the enterprise service bus. Once the application logic, for example a public endpoint, is breached the attacker may gain sufficient access behind the outer firewalls to continue to breach the whole network. The introduction of horizontally scalable systems into enterprise architectures requires a radically different approach than the traditional one. The introduction of IoT-enabled devices, smartphones, and digital platforms that all handle personal data governed under the GDPR, suggests that the traditional passive security methods cannot be considered appropriate security. As determined in chapter 5, to assess the appropriate level of security, account shall be taken of risks presented by data processing. For example, provided the communication over the enterprise service bus cannot be analysed in real-time, while the company is still able to send and receive user data in real-time, then the appropriate level of security should not be considered achieved. If an attacker gains access through such a public end-point, it may mean the attacker also gains direct or indirect access to the data store. Thus, the monolithic architecture for scalable systems with public end-points may be considered problematic from a security point of view.

IoT security is also an issue that currently faces a challenge in scaling with the explosive growth of IoT-enabled devices (e.g. home monitoring cameras) (Pulkkis et al. 2018). This is considered due to their reliance on a centralised update service and a device-required configuration (Kshetri 2017). This centralised governance architecture may act as a bottleneck or point of failure that then disrupts the entire network. Other attack vectors such as vulnerability to distributed denial-of-service attacks, hacking, data theft, and remote hijacking also exists. In this thesis, we are primarily considering IoT-devices when they handle personal data, for example wearable devices, webcams, home automation/security systems, or digital personal assistants, but their security concerns a broader perspective. Malicious IoT-networks (called botnets) have become a threat to the information society and although botnets are not necessarily handling personal data, their vulnerabilities influence security in other systems handling personal data. The IoT-architectures tend to be distributed, while the system governance can be centralised or decentralised. A similar distributed architecture can be found in scalable systems that for example employ microservices. In our view, decentralised system governance tend to work better for distributed architectures than centralised.

Based on the discussion above, we can identify three main categories in monolithic designs that can be differently addressed through decentralised systems.

Application logic
Data management
System governance

The use of microservice architectures (cf. chapter 2) to create scalable systems potentially enables the system operator to both localise problems and to improve the creation of autonomous security supervision. Using the three categories above and combining with analytics objectives for IT-security, a framework for handling and improving security in scalable distributed architectures is presented in Table 6. The framework offers an overview of how active network security can be a solution for achieving the status of "appropriate security" as the general data protection regulation loosely defines.

A current challenge for organisations in using distributed architectures e.g. a platform based on microservices, lies in how authentication and authorisation for each microservice is handled. The de-facto industry standard for handling authorisation is OAuth2 (Hardt 2012). The authorisation challenge for different architectures can be described as data traversing in the non-scalable monolith often between point-to-point, in the scalable monolith often as point-to-multipoint, while in the decentralised system (e.g. microservice, mobile, or IoT architectures) data may need to flow multipoint-to-multipoint. The challenge with OAuth2 is that it delegates security concerns to the SSL protocol. This means that the client authenticates the server by using the provided SSL certificate. As the server does not authenticate the client, this means the server has no way of knowing who is actually sending the request. In data flow architectures this may be problematic as it may lead to for example man-in-the-middle attacks. However, because of the challenge new solutions that improve upon existing solutions have been proposed that instead use decentralised authorisation technology (e.g. Crary and Sullivan 2015; Moffatt 2016). For example, by utilising the blockchain as an authorisation backbone infrastructure, devices can potentially communicate securely, exchange data with each other, and perform transactions automatically by using smart contracts. Currently a major factor impeding this development is related to the processing throughput of blockchains. A current emerging research area is how to other types of distributed ledgers or how to modify the blockchain workflow through the use of state channels for the verification of state changes outside the blockchain, and then registering only a minimal record on the blockchain for forensic purposes.

Table 6 - Analytics-based Framework for Active Network Security

Analytics Framework for Active Security in Scalable Architectures				**Analysis**	
	Application layer	Data management	System Governance	Input	Output
Descriptive analytics	-Quantify historic application usage patterns. -Identify anomalous patterns.	-Quantify historic data store access patterns.	-Quantify historic scaling patterns, internal network patterns, and instance access monitoring.	-Historic data.	-Pattern recognition models.
Diagnostic analysis	-Provide a near real-time anomaly threat analysis of deviating usage behaviour, using adaptive models based on descriptive analytics. -Provide active intrusion management, by monitoring the techniques described in section 5.3.	-Provide a near real-time threat analysis of deviating access behaviour, using adaptive models based on descriptive analytics.	-Provide a near real-time resource analysis of deviating instance behaviour and instance access, using adaptive models based on descriptive analytics.	-Real-time data.	-Alerts.
Predictive analytics	-Forecast trends in usage behaviour and determine potential oncoming peaks that can disrupt the service, e.g. a Denial of Service attack.	-Predict access behaviour, both on user level and on data store level. -Classify deviating behaviour that indicate oncoming malicious data transfers.	-Predict instance and system failure. -Forecast deviating behaviour that indicates oncoming malicious system behaviour.	-Real-time data.	-Signals based on probability.
Prescriptive decision making	-Application alerts or signals are activated, then initiate autonomously specific decisions from the governance rule set, e.g. refuse access to the service for a specific user or redirect request to a honeypot installation.	- Data mgmt. alerts or signals autonomously initiate specific decisions from the governance rule set, e.g. aborting a data transfer or revoking user access to data store.	-Defines a rule set of generalised decisions to mitigate the effect of attacks, e.g. revoking system access or starting more instances to cope with increased processing load. -Maintains an operative overview for the system of decisions taken.	-Alerts and signals.	-Decisions.
Forensic analysis	-Record all user interactions with a service in a user-transparent way in an immutable data store that is only accessible for forensic purposes and where data is either encrypted, pseudonymised, or anonymised.	-Record data store access, actions, and data transfers in an immutable data store.	-Record system access in an immutable data store. -Provide forensic analysts with access to user interactions, data store forensic data, and system data. -Provide methods to analyse said data.	-Real-time data.	-Historic data.
Visual interactivity	-Provide a human operator decision support through visual overviews of analysis methods above, incl. specific behavioural views of different type of actors in the system. -Interactive ability to act on non-automated alerts or decisions and to launch new analysis efforts.			-Real-time and historic data.	-Visual interaction.

7.3. Platform Privacy Regulation

Thus far in this chapter we have examined which security measures companies can take to appropriately secure their information systems and how the GDPR holds up in a technical environment driven on by the development of intelligent services. The final section will look towards the data driven economy that supports digital platforms, to explore some future policy options. It should be noted that the discussion is targeted at incumbent large-scale platforms offering intelligent services and is not applicable to every website. This follows a similar classification as that which been defined in the GDPR regarding the requirement of appointed data protection officers in certain organisations and in the NIS regarding whom it applies to. The section focuses on the following research question:

RQ 3. What is a potential future direction for EU privacy regulation in guiding the continued development of digital platforms?

The challenges that face the individual's right to privacy are substantial. Some ten years ago, data was first termed as the oil of the digital economy (Palmer 2006). Today, user generated data has arguable become the currency of the virtual world. The more complete and timely data we have about an individual, the more it is also worth to a service provider and particularly a platform provider. Complete data is here defined as accurate, but also as encompassing and in-depth as imaginable. Determining the exact worth of user data is difficult, as the intrinsic value is dependent on many factors, such as type of data, accuracy, timeliness, and uniqueness. In addition, the market value depends on factors such as the ability of the company to create insight based on the data, connect the data subject to a service market, and then monetise upon these earlier findings.

The difficulty in determining user data valuation and setting a standardised price for customers led for example Google to create an auction market, AdWords,[53] for selling targeted advertising based on consumer activity to third parties. The auction market allows Google to create a dynamic pricing logic that self-regulates based on demand and availability. Many other platform companies today (e.g. Facebook and LinkedIn) have a similar model or a variation of the model in use.

Although we today may consider our ability to a private digital life impractical and unmanageable, it is likely we have only taken the first step on the digitalisation journey. Estimates by IDC on behalf of the EU Commission considers the data driven market in the EU for 2016 to roughly amount to 2% of GDP. [54] Under an

[53] See the official Adwords documentation, accessed 29.10.2017 https://adwords.google.com/home/

[54] See European Data Market (SMART 2013/0063) Final Report, by IDC and Open Evidence for the European Commission, published 1.2.2017

increased investment scenario, the data driven economy is expected by IDC to more than double until 2020 (in absolute numbers from € 300 B (2016) to € 739 B (2020)). Sectors that become data driven can offer double-digit growth for the near future, something the EU economy acutely needs. The EU Commission's strategy for a digital single market is an important effort in propelling companies to invest toward becoming data driven. As the platform companies have shown, the platform can be a very efficient business model for accumulating personal data and to profit from the interaction of market participants. However, the current business model for data subject facing platforms also raise many questions and fears, both from a data protection point of view and societal impact. To mention two common mischiefs; does the platform misuse personal data, including insights based on such data, and how do platform companies contribute to the local society where the consumer resides, in for example local tax returns.

Economic research into platforms may yet have to conclude how to value user data in relation to a platform. For antitrust cases Grunes and Stucke (2015) highlighted the problematic relationship of free services that are paid in user data, but where user data have no determined value. The value of collected user data can be estimated in individual cases by any current or future service that may entice the user to continue using said service. Therefore, it can be argued that existing user data should always be considered of value, even if left unprocessed. Grunes and Stucke (2015, p.7) probe the question why companies would otherwise continue to "*spend a considerable amount of money offering free services to acquire and analyze data to maintain a data-related competitive advantage*". User data in a digital format bears at least the cost of the research and development that has gone into implementing said platform. Perhaps more importantly, in practice, the value of user-contributed data is best determined by the value it provides the company which accumulates the data, to create a barrier of entry towards future entrants. A comparison to Facebook's acquisition of WhatsApp and the later allegations and consequent fines imposed from the EU Commission of non-transparent activity on behalf of the acquirer during the acquisition process can be made (Lunden 2014; White 2016; European Commission 2017). Acknowledging that all personal data has a monetary value, although indeterminable in a generalised way, may also improve the ability of regulatory authorities to consider platform privacy in anti-competitive terms.

Privacy in general is of immense importance in improving our trust towards the digital society, but particularly so in a world where we are striving to create intelligent services that can advise us humans what to do or even act on our behalf. Still consumers are saying that privacy issues are a great challenge and that 44% of consumers do not trust the companies or platforms behind today's digital platforms

and services with their personal data. [55] When personal data are used for creating insights about users and then traded forward for profit (supported by privacy policies), it can cause users harm. Pew Research (Smith 2014) found that in a large majority of cases exploitation of user data causes uncertainty and that confidence in service providers is weakened. Therefore, it should be highlighted that the Regulation is not only one dimensional, in the sense that its existence is to only guarantee the protection of the data subject. Rather the Regulation also offers a notion of long-term business opportunity, if realised correctly, by improving the consumers trust in companies and their platforms/services. Future Internet of Things-enabled platforms are likely to record anything (behaviour, voice, video, and other special categories of sensitive data) that occurs in the consumer's personal space (e.g. private residence). It should then become evident that these services will need the trust of the consumer. The more encompassing the data that is being processed regarding the data subject is, the greater the importance of how privacy and consumer choice regarding the platform is regulated becomes.

Early influencers on the design of privacy preserving information systems, defined the task to accomplish as "The Path to Anonymity" (van Rossum, Gardeniers, and Borking 1995). We also find that the current EU rational for data protection is based on the premise that anonymity is plausible and desired. The European Convention on Human Rights, Article 8, has been interpreted as equivalent to a right for anonymity for a natural person. The design rational presented by van Rossum, Gardeniers, and Borking (1995) explores a number of potential techniques and how privacy enhancing technology can be employed in information systems. Although the technological jargon presented in their work is still mostly accurate, from a modern digital platform development point of view we consider the anonymity target as a utopian objective. At the time, information systems were mostly closed off and user data was very costly to store. Whereas today a state-of-the-art digital infrastructure is often described as an evolutionary entity that employs generative mechanisms in its inner workings that determine its success over time.

Based on our reasoning, we formulate three theses that we consider should be the leading indicators for data protection platform legislation when it comes to the consumer-business platform relationship.

1. Every networked device is inherently vulnerable, i.e. leaking information, but some more than others.
2. All personal data can be assigned a monetary value and data describing the data subject will be stored for an indefinite time, and data will eventually be processed.

[55] For further details see http://www.trustarc.com/blog/2016/01/28/state-online-privacy-2016/. Accessed 29.10.2017.

3. Privacy does not equal anonymity, as there cannot be true anonymity in a near-fully connected world.

In chapter 6 we posed a question regarding how trust can be created for digital platforms, we think that the following definition of privacy could regain and keep the individual user's trust in digital platforms:

> Privacy should be a right for each data subject to continuously monitor and actively participate in the control of where and how data pertaining to the individual is stored, handled, consumed, transferred, and erased. Additionally, any personal data collected through the use of the platform, should be monitorable and controllable through the same platform. The same applies for any insights gained by using personal data collected through the platform by the platform operator or by a third-party service.

When considering the traditional digital services offered on the Internet the GDPR offers a relatively good balance between data subject privacy and company profiting, but when considering the platform model we find the GDPR relatively limited. The remainder of the section focuses on elaborating on this inadequacy and providing detailed suggestions for improving platform privacy.

Today, data subjects are often completely exposed to platform providers, and there is often little or no privacy in regards to a handful of global companies. As contended in chapter 6, this is enforced through complex privacy policies were users are forced to give up their rights and data protection laws are circumvented. These companies have gone to lengths to create as complete registers as possible on their users. For example, this has been achieved by creating data collection syndicates for registering information from not only their own service, but also when a data subject uses the services of other companies that implement the same technology. [56] So far, the gathered information mostly contains behaviour related data for direct marketing purposes, but future development is not limited to this. Automotive companies (e.g. Tesla) have launched semi-autonomously driving cars that work by accurately scanning the surrounding environment, which the companies then want to monitor continuously. For example, fleets of these cars would very effectively be able to police fellow road-users, by reporting to authorities which registration numbers has passed by, the speed of other cars, and distances between cars (cf. public interest analysis). The introduction of new Internet of Things data sources

[56] One such example is Google's Display Network that employ a technique referred to as Remarketing, which uses cookies placed in a user's web browser by other websites to track the users earlier web history. According to Google's own marketing material: "*With millions of websites, news pages, blogs, and Google websites like Gmail and YouTube, the Google Display Network reaches 90% of Internet users*". Accessed 31.10.2017 https://adwords.google.com/home/how-it-works/display-ads/

(or data generators) makes it even more important that data subjects are given comprehensive control of data related to them in near real-time. Our definition of platform privacy focuses on the data subject as an active actor, who can and should make a conscious decision regarding how privacy should be invoked also after that the consent contract has been signed. The definition is motivated by the data subject's capacity and capability to choose an alternative platform service approach, which we find is lacking in the current Regulation. Forcing companies, which have already achieved a de-facto monopolistic or oligopolistic position through their "processing silo" platform, to truly open up user-generated data would, in addition to improving privacy, also lead to an improved competitive digital landscape in Europe.

7.3.1. Competition and consumer choice in the data intensive business

Although the digital platforms have improved their practice regarding personal data portability since we authored the original paper (Westerlund and Enkvist 2016), the underlying issues with competition and consequent limited consumer choice in data intensive business, still exist. In the previous sections, we argued that the network externality effect contributes to create de-facto monopolies in the digital world through the creation of "processing silos". We consider the fundamental reason for this to be the immobility of data among platforms. Data immobility provides incumbents with an entry barrier against new competition. Data immobility includes user identification, user data, and user profiles. Cerf and Quaynor (2014) made the argument that "*a fragmented Internet that is divided by walls will inhibit the free exchange of ideas, increase business costs, stagnate job creation, and fundamentally disrupt our most powerful global resource*". The near non-existence of consumer initiated data sharing between platforms highlight this problem. Today, user contributed data are often locked in behind a service gateway that is connected to a platform user ID. An open flow of data implies that service discovery and service linking can be initiated by the data subject. The GDPR requires that the platform allows for transportation of personal data away from the platform (or service), but the GDPR does not force platforms to allow for the open flow of data to and from their platform. At the time of writing this thesis, many companies have implemented functionality for data subject initiated transfers of personal data and some even provide public API's in anticipation of being compliant with the GDPR requirement on data portability. The requirement for platform companies to be compliant with the GDPR on data portability has perhaps become one of the most significant disappointments for entrepreneurs and privacy advocates alike.[57] The opinion

[57] See for instance Madge, R. (2017). GDPR: data portability is a false promise. Accessed 5.11.2017 https://medium.com/mydata/gdpr-data-portability-is-a-false-promise-af460d35a629

presented by the Article 29 WP (2013, p.47) promised what can be described as an open flow of personal data, the "*direct access to their data in a portable, user-friendly and machine-readable format may help empower them, and redress the economic imbalance between large corporations on one hand and data subjects/consumers on the other*". In the analysis of the finalised Regulation the Article 29 WP (2016) concludes that only data that have been directly and actively provided by the data subject (including observations such as previous history) are to be portable and that the Regulation aims to produce interoperable systems, not compatible systems.

This change in opinion certainly reflects some of the challenges that the legislator went through in the enactment of the GDPR. Although certain global platforms may need additional regulatory incentives, the GDPR was perhaps not the best place to include such platform specific legislation. With the exception of some global platforms, most organisations handling personal data today would likely struggle in implementing an open data flow. Thus, portability as an open data flow should be seen as a directional effort for the future, not as a lost cause. To consider the needs of start-ups and other new innovating ventures, the EU should continue to work towards the vision of open data flow. This will become an ever more important issue for the future with the introduction of intelligent services, such as personal digital agents.

As stated earlier, many platform providers have or are beginning to open up portability APIs, but to achieve true data mobility we believe a clear legal requirement is a necessity. An initial step in regulating platforms is a mandatory separation of personal data storage activities and the platform service provider (processor) duties into separate legal entities, as this would create a possibility for actual personal data control. As considered in section 7.2, the transformation of IT-architectures from centralised to decentralised, should be transferred to the platform business model as well. An abundance of providers will improve data subject privacy and markedly improve the start-up landscape in areas that are now dominated by incumbent platforms. That services of similar nature could conform to the same data-sharing standard is plausible from a technological perspective, but other interests (e.g. incumbent business and sovereign) have so far prevailed. As an example, current social network platforms share a common data structure, largely based on messages, user IDs, and relationships. Standardising such a social networking platform should be comparatively straightforward, compared to for example the standardisation efforts surrounding mobile communication networks such as 4G mobile networks. [58] However, standardisation will most likely not drive the centralised platforms towards an open data flow without a regulatory requirement, as this may also mean creating a competing decentralised business model whose popularity will be based on consumer trust and loyalty. It should be

[58] Standardization efforts for social networks is currently ongoing in the W3C Social Web Working Group. Accessed 5.11.2017 https://www.w3.org/wiki/Socialwg

noted that the problem described here is not connected with the existence of current platform companies, but rather in how their business model is defended. By transforming the current centralised platform business model, any of the current incumbent platforms can continue being successful, but this transformation to open up the processing silos will likely require Regulator intervention to transpire. In addition, consideration must also be given to the fact that the decentralised business model in itself may also develop to resemble the current centralised model without guidance. Thus a platform regulation that demands the open flow of data may have a positive influence for both the centralised and decentralised model in introducing trust as a key-design goal. The EU Commission has a long and often successful history in providing regulation aimed at opening a closed market; this can perhaps best be evidenced from the opening of the telecom sector. Continued focus by the EU Commission on open data flow in connection to platforms is needed.

In an earlier section, we stated that the legislation sets unreasonable expectations on the data subject when it comes to managing given consent contracts. By separating the data storage activities into a separate legal entity, new service innovation can be established in personal data storage solutions (data store). In extension, this should lead to a generalised solution where service providers would allow any data store provider to provide the personal data store backend to a service. Then by using personal data store providers, consumers would have a natural way of storing and controlling all their consent contracts from a service. This solution allows the user to determine the service and security level in a much more fine-grained fashion than today. If the data subject wants to continue with a similar setup that exists today it would be possible, a platform service provider would likely pay the potential transaction cost on the user's behalf in return for non-restrictive access to processing the user's data. Conversely, privacy-aware customers would have an option as well if they want to pay themselves. New business ventures could get access to personal data and thus compete on equal terms.

To enable the vision of consumer initiated open data flows, identity management needs to be handled in a different way than today. Centralised identity management needs to give way to decentralised solutions. A federation-based decentralised authentication service is already in use for a worldwide roaming access service called Eduroam, where access is handled in a similar fashion to email identities "user (at) domain".[59] Eduroam was developed for the international research and education community. The EU project FutureID developed a decentralised system for exchanging user ID credentials between different Internet services (Bruegger and Roßnagel 2016). Javed et al. (2017) propose a framework for cross-domain identity and discovery to perform web calling services based on WebRTC. These three solutions are built on the premise of trust, however, but also trustless consensus

[59] See https://www.eduroam.org/ for further details. Accessed 5.11.2017.

solutions based on distributed ledgers, such as the blockchain, have recently been proposed (Xia et al. 2017). These initiatives show that technology is becoming mature to support a more user controlled privacy scheme that would support data mobility between platforms and services. What is missing are incentives for incumbent platform providers to open up their platforms to decentralised services. Essentially, once a platform becomes a de-facto standard, a separation of the platform and the data store is needed to allow for continued competition in the field. User data can be moved in accordance with the original platform, while processing takes place in differentiated services.

7.3.2. Resolutions to the Centralised Platform Concerns

To define a future direction for Europe in how to deal with digital platforms, the thesis has followed Brynjolfsson and McAfee's (2014) recommendation that we need to define "*what we really value, what we want more of, and what we want less of*". We have made an argument for modifying the Data Protection rationale from a focus on the right for anonymity – towards a Data Protection rationale based on individual and active control. An insight gained has been that if we want to achieve a safe digital societal inclusion, we also need a bridge between privacy policies, business models, technology standards, and legislation. As highlighted throughout the thesis, these are currently often on opposite sides of each other, whereas a balance is the key to creating a digital society that people can trust. Below follow three resolutions for consideration in a future EU platform privacy regulation that we find would clarify the data subject's position in regards to platform privacy issues, particularly so when intelligent services based on artificial intelligence become as commonplace as for example email is today. The ability for the data subject to choose between different providers of intelligent services, e.g. intelligent personal agents, and have them connect to the user-initiated open flow of personal data, will be key to a digital society that is trusted by the EU residents. The resolutions should also strengthen the competitive landscape, particularly with a focus on improving conditions and ability for new diversified digital ventures and start-ups to challenge incumbents. When the EU residents trust the digital environment, that business environment is also likely to grow at an even more advanced rate compared to an environment that is neither transparent enough nor allows for consumer choice.

7.3.2.1. Resolution 1 – User lock-in

One of the central resolutions of how platforms are regulated ought to be aimed at lessening the ability of incumbent global actors to lock-in the user base to their platform. Our motivation is to enable true competition and a selection of differentiated services. The de-facto platform monopolies create a dangerous future where a few companies can dictate or influence how the digital communities should

behave as well as follow up how they actually behave. Once again, considering intelligent services that may soon become so smart that they even act on our behalf, if we allow for an environment where there is only one platform offering a specific service, then everyone is required to conform to the behaviour of this service. One possible way to avoid this lock-in effect is to regulate the company-internal information sharing between all services with a public audience. Unless comparable public data sharing protocols (APIs) exist that conform to a sector-based standard (incl. service discovery, service linking, and data structure), any internal information sharing would not be allowed between said services. This, however, with the exception of some internal identity authentication and billing services that the company may not want to expose. These public data API´s must have the same service level in regards to reliability, extensiveness, and promptness as any internal information sharing protocol.

Essentially this entails that for example a platform such as Facebook would not be allowed to share data subject generated data between e.g. WhatsApp and its other services without a public API (incl. service discovery, service linking, and data structure) for accessing the flow of user contributed data through the API. Argenton and Prüfer (2012) suggested a similar solution also for regulating search engines. Their argument was that the best way of dealing with Google's dominant position in search engines, would be to force it to share its search data, such as previous user searches and clicks, as well as other important metrics.

7.3.2.2. Resolution 2 – Authentication and data stores

The second resolution we put forward is regarding identity authentication and data stores, essentially re-defining how, when, and why data are transmitted outside the data store. To limit the current unwanted tracking ability of data collection syndicates, we propose that any authentication and data storage of personal data is separated from other processing activities. By separating authentication and data store into a separate legal entity, it opens up for innovation in new types of decentralised authentication and data storage solutions. By requiring a monetary based (not data based) transaction cost for the identification service, paid either by data subject or intended service provider (controller), it will be possible to open up innovation for new types of services that offer alternatives to incumbent solutions that are built on the premise that cost is paid directly or indirectly in user data.

By implementing a requirement for an external data store as the backend for personal data, the identification of users from other services must be addressed in order to define relations between individuals. The ability to contribute and act under a pseudonym can also be issued by the data store. Ullmann et al. (2015) [60] suggest a

[60] Cryptographic algorithms exist for this purpose and have been suggested e.g. for broadcast purposes in the automotive industry to ensure privacy. For more information see: Ullmann et al. (2015).

cryptographically sound approach for handing out time-limited pseudonyms. This approach could be extended to the data store that would offer data subjects pseudonyms, which could unlink provider control and sensitive data misuse by other parties, while the data store would still be able to store any historical records on the behalf of the data subject. Unlinkability of messages in a system means that the ability of the service controller (or attacker) to relate these messages to an individual do not increase by observing the system over time (Pfitzmann and Hansen 2010). We find it essential to assure an ability of sender anonymity and message unlinkability in regards to the controller; in case of misuse, authorities can still gain access to the true identity through the data store. The data store provider would thus be able to designate a pseudonym ID to a data subject upon request, which when used can have a certain level of similarity to the true User ID, but offers a way to obfuscate certain easily identifying details about the data subject. A data store would also likely be offering network services, e.g. virtual private network (VPN), in order anonymise access to a public network. The resolution above should also ensure that the ability of a controller profiling of children, intentionally or unintentionally, can be reduced. Device or browser fingerprinting may still be an issue, but in the case of the browsers ability to offer privacy settings or privacy modes that implements some obfuscation mechanism or reduces the information in the browser fingerprint so that the fingerprint can no longer be considered unique, should hinder unwanted tracking.

7.3.2.3. Resolution 3 – Security and data protection policies

The third resolution we are proposing is in respect to how security and data protection policies are reviewed. Achieving complete security is as improbable as achieving full anonymity; too many attack vectors exist to be able to mitigate them all separately. Nevertheless, the importance of dealing with security breaches in a proactive and reiterated fashion can never be overstated. The Regulation introduces a new role of a company-located data protection officer in addition to the supervisory authority. The role requires 1) expert knowledge of data protection law and practices, 2) being in a position to perform their duties and tasks independently, and 3) liaising with regulators over personal data breaches and 4) monitoring the performance of the data protection impact assessments of organisations. The data protection officer is a mandatory position in organisations that fulfil certain criteria, the role can initiate internal security and policy auditing and is a first and important step. The role, although not formally, may require a law degree for fulfilling the description of a data protection officer. The role is similar of a financial officer that also needs a formal financial reporting background. As stated earlier, we find there is a gap between the law and its practical implementation. Security and data protection technology are highly complex technological subjects. We find it improbable that a supervisory authority can markedly improve the consumers' trust in IT-services on its own. To certify a company for how it handles security and data

protection requires in-depth engineering skills. We therefore propose a third party auditor role that periodically monitors security and data protection in companies. In practice, this would take the form of a compulsory and periodically returning review by auditing, in a similar fashion to a financial audit, where the auditor is responsible for expressing an opinion. The auditing opinion indicates that reasonable assurance has been obtained, that the statements as a whole are free from material misstatement, whether due to fraud or error, and that they are fairly presented in accordance with the relevant technological and legal standards (PWC 2013). If it is found later on that an auditor neglects their legally stated duties they would be held liable as well.

7.4. Discussion Summary

The aim of the discussion has been to extract answers to the research questions posed. The underlying drive for the thesis has been to improve the understanding of the transformation that platforms have on the digital society, particularly so through the lens of the agreed upon human right to privacy of one's private communications. Towards the end of the writing process, the focus has been on how trust can be achieved in the digital society. As earlier reported, nearly half of the population does not trust current solutions. Without the data subject's trust, the deployment and uptake of coming intelligent services will become more difficult to achieve.

7.4.1. Summary of Research Questions

A summary of the answers to the research questions is presented below in the format of main key points, for the elaborated answers see the previous discussion.

RQ1: What are relevant interpretations and ambiguities for information systems that can be derived from the GDPR, particularly in regards to such processing of personal data that leads to profiling and automated processing?

Two core information system design implications stemming from the GDPR is to ensure the implementation of the concepts of data minimisation and data protection by design and default.

These concepts have been shown to go against both the nature of today's vertically integrated platforms and most importantly against the innovation intelligent services may bring.

- The concepts offer a relevance for traditional standalone services that do not have the strategic aim of becoming a platform, but as for protection against growth-focused services and platforms the concepts offer rather miniscule protection.
- These concepts should be updated to focus on a clear legal requirement for controllers to provide and maintain means for data subjects to actively

control the processing of personal data, including third-party transfers and processing that occur in relation to the platform.

The need for transparent processing, including transparent data transfers, manipulations, and removals, may be best met by an immutable forensic data storage solution, for example a distributed ledger.

- Treating each corresponding data operation as a transaction and recording that transaction, offers an auditable record for forensic purposes and an approach for showing compliance to potential data subjects and the regulator.

Client-side processing and processing data on virtual identities have been identified as ambiguous areas in the GDPR.

- The view presented here is that both methods should be bound by the GDPR, but in practice this is unlikely to occur.

From a data protection perspective client-side processing should be considered the preferred method for intelligent service provisioning.

The GDPR limits the use of information systems processing personal data that are using the following methods:

- Fully autonomous agents or decision making.
- Some machine learning algorithms, e.g. those trained with unsupervised learning or reinforcement learning methods, provide a difficulty in determining the behaviour of the algorithms and this may create a transparency problem. For example, unsupervised learning may contain clusters that represent information in an unsolicited manner, as clusters may be a synthesised product of special categories of personal data such as religion, race, sexuality, or health. Now the processor and/or controller may or may not know this as a fact, but this has a clear implication on the creation of profiles on data subjects.
- Due to deep learnings sensitivity to training data tampering, assurances must be made of training data integrity, particularly when group learning is performed.
- All machine learning techniques are also susceptible to stereotyping and bias due to the training dataset, and under/overfitting of the model, thus the use of these techniques requires assurances from the controller that output is not offending and that some transparency exist in regard to a resulting decision, e.g. which data have been used as input.

RQ2: What future technical implications can "appropriate security", defined as a legal requirement for lawful processing under GDPR, entail for scalable information system architectures?

As data protection is sometimes misunderstood as only dealing with misuse that occurs through malicious intent by the controller or processor, an aim of

the thesis is to broaden the discussion towards how security is handled in companies and to examine what should be considered appropriate security from a generalised technical perspective.

An important aspect of the GDPR is to address breaches of companies' security and consequent leakage of their users' personal data. A technology agnostic law that can stand the test of time, offers little guidance towards what measures should be taken to achieve compliance with the regulators intentions towards appropriate security.

Determining technological actions based on achieving an environment that ensures appropriate security, may be challenging for controllers, processors, and owners of information systems. The regulators focus on data security methods (e.g. data minimisation and privacy-by-design) is understandable, but from a technical perspective appropriate network security is just as important. The omission of what can be considered guiding network security principles in the GDPR should not lead to a lesser focus from companies on improving this aspect of their information systems.

GDPR recommends as a minimum precaution that personal data be pseudonymised before being stored, particularly if data are stored long-term. Where possible, the controller should try to anonymise data belonging to a special category. This implies for example that such traffic meta-data that is not needed for service personalisation, but where data can be used at a later stage for some other purpose, should be anonymised.

- Meta-data describing, e.g. data source, access rights, and justification for lawful processing should be recorded along with the data when it becomes associated with a natural person.
- Client-side processing, particularly profiling activities, may be more secure as data would only be stored in a readable format locally when needed, and that it otherwise remain encrypted (incl. an encrypted backup in the cloud). Thus, vulnerabilities to such systems would affect devices on an individual basis. However, in client-side processing the role of who, if anyone becomes processor, is ambiguous and leading to a difficulty in determining the requirement of lawful processing. Our view is that due to the added security, this type of processing is preferable in many cases, particularly for data from real-time based interactions that is used for the execution of machine learning models.
- Machine learning algorithms usually needs data in an unencrypted form. Consequently, if a controller or processor is located in a third-party country without a data protection agreement with the EU and maintains root access to nodes, then any software stack can be considered unsecure for processing personal data. This applies to any type of node e.g. cloud, mobile, IoT or desktop.

Integrating tools for big data analytics into the security workflow offers novel opportunities for detecting intrusions or unauthorised data access. Implementing an active network intrusion detection system based on machine learning techniques offers companies today a relatively effective way to improve security in their networks. Open-source big data analytics solutions offer a cost efficient way to improve security.

- In our experimental MapReduce implementation of ELM we could determine that it scales horizontally and that it can be used for network intrusion detection with a relatively high success rate. Using the Hadoop tool, we also show that machine learning based intrusion detection using ELM can scale to large datasets using the MapReduce programing model.
- An insight gained during our research is that the main challenge companies will likely face, is in determining what data should be recorded and how to label the training set to create a detailed and specific representation of potential threats the individual system can face. Rule-based intrusion detection tools can be used as a first step in generating a company specific dataset. We also present an alternative method by designing and inserting data generators into web software installations.

We examine the research question as how to define "appropriate security" through the hardening of an installation of WordPress and the creation of an active intrusion detection methodology for the WordPress system. The focus of our study was on mitigating effects of automated scripting attacks. The active network security method presented offers the system administrator a path towards active defence against malicious attacks. Combining the use of data generators and analytics to create an active methodology should be particularly useful against fully automated attacks where the attacker is not targeting a specific system, but rather scans the Internet for any potential target. Furthermore, our data generator method offer machine learning based network intrusion detection a novel way to create labelled training data. This offers the opportunity of further exploration in the use of big data in network intrusion detection, defence, and forensics.

RQ2.1: With focus on security in publicly accessible software, what is a viable technology basis for a scalable processing architecture?

The thesis has highlighted the currently ongoing shift in information systems, whereby centralised platforms are starting to shift toward their decentralised counterparts and technology is shifting from the monolith toward distributed architectures.

- An objective with the research question is to understand the technology stack and methods behind big data analytics, as well as to elaborate design

concerns and security by implementing an architecture for a big data analytics processing tool.

The ability to create intelligent services using models based on machine learning techniques opens new business opportunities. If the intended use requires massive processing power, e.g. for individual model training or transfer learning per user, then this will require a massively scalable processing architecture.

The practical use of analytical systems typically require them to be scalable. One important factor to become scalable is the ability to grow the processing environment when required, and shrink the environment when resources are no longer needed. To achieve this elasticity, a public cloud is often used. This architecture opens the system to new network and data security threats that need to be mitigated, as reported for RQ2.

In our results we present an architecture suitable for processing spatio-temporal data, including processing on both historical data-at-rest and streaming data. Our findings are that scalable processing architectures can be implemented efficiently through a generalised worker/master node architecture, where the master-node performs a type of scheduling duty. The architecture designed was modularised and this offers the ability to run these modules as self-contained microservices.

- An important part of data security in the GDPR is data provenance, i.e. authenticity and integrity of data used for analytics, and this also applies to model output. An aim has been to investigate ways to achieve service integrity for model output as well, which can also be transferred to an autonomous production-level system. Thus the training process developed was fully automated by making use of both a verification dataset and an evaluation out-of-sample training dataset for calculating model error rate, whereas model output techniques such as ensembles, model selection, and model management (replacing bad models with new improved ones) were used to keep results stable and to improve results.

Scalable architectures for platforms can be implemented in various ways, e.g. as a centralised or as a decentralised system. Based on referenced examples, the monolith architecture may make it more difficult to monitor, to detect intrusions or other attacks, and to remediate attacks. The microservice may offer a better ability to compartmentalise security issues due to the modular nature and that each module has a well-defined role. Provided governance is decentralised then security governance should become more manageable. In Table 6 "Analytics-based Framework for Active Network Security" we present a solution for ensuring appropriate security in connection to RQ2.

The use of microservices can support the personalisation of intelligent services, this includes the ability to handle individualised back-end services

for client-side processing. Our explorative case study detailed a generalised modular design that can be autonomous and scalable to a large extent. The handling of scalability and security governance should remain in the microservice module. The initialisation and shutdown of microservices could for this purpose be connected to a decentralised external governance mechanism that also maintain billing, authentication, authorisation, and other core functions. For this reason we refer to the system as decentralised and not distributed.

For RQ3: What is a potential future direction for EU privacy regulation in guiding the continued development of digital platforms?

The author considers the GDPR as a much-needed improvement to the current Directive and a great leap in comparison with many other countries' legislations. However, the Regulation also includes a rationale based on anonymity that is impractical at best and unfeasible at worst. The Regulation may consequently be rather toothless in compelling and incentivising platforms to become transparent.

- Introducing IoT into the home will in time digitise any personal experience occurring inside the walls of private property. The GDPR highlights the importance of data minimisation and privacy-by-design, hence the clash between the technological and legal views are obvious. Regulating digital platforms that offer intelligent services is important if we want to remain private in our own homes. However, anticipating the challenges is a very difficult task.

The centralised governance model is the common manifestation of the platform today and we discuss its challenges for society at large by being so effective and impeding nearly any competitive alternatives. We highlight the benefits of user initiated open data flow and the ability for data subjects to choose between multitudes of service alternatives.

Open data flow entails the innovative use of personal data stores that offer various additional methods for data subjects to improve their privacy, e.g. transparent data access records or a pseudonym identity service.

- To create an environment for open data flows we propose three resolutions: break the lock-in ability of incumbents, unlinking authentication and data store from other processing activities, introducing mandatory and continuous security audits.

The existence of service alternatives will become an even more important issue when intelligent services, such as personal intelligent assistants, arrive en masse. Current processing silos maintained by many incumbent platforms are an impediment to a diversified development that guarantees start-ups equal opportunity and democratic rights for data subjects.

To regulate the centralised platform's ability to sustain a processing silo we need to consider both the organisation and the logical communication. Requiring compatibility among systems in connection to the platform is the key to dismantling the processing silos and allow for decentralisation and true competition to occur. Similarly, when the EU Regulator considers how to introduce laws governing artificial intelligence, the first step is to solve how companies other than current incumbent platforms can get access to data. A proliferation of intelligent service providers is important if we value our democratic rights in the future.

The ability to construct decentralised platforms is not tied to the development of distributed ledger technology. The rapid development of distributed ledger infrastructure for constructing decentralised platforms has shown that the "code is law" principle is a complex proposition that needs more time to develop secure design patterns. Although it solves the trustless consensus dilemma elegantly, trust-based solutions will likely continue to be the drivers over the foreseeable future. Our resolutions do not make a distinction, but rather applies to both types of solutions.

At the time of writing we can but speculate that to achieve compliance with the GDPR, platforms will seek to establish lawfulness of processing through contracts. The stringent conditions that consent requires, will likely be reserved for processing special category data or profiling that leads to a legal effect. As stated, the ability for platform companies to create intelligent services will require complete past and present data in regards to the data subject, and for this equivocal purpose consent will be difficult to obtain. Thus, via a terms of service agreement seeking to establish lawfulness through contract, a platform company can obtain wide-ranging concessions to process personal data collected through the platform as it sees fit.

In the thesis we assume that the invasion of the data subject’s privacy is a measurable property and not a binary value. The measurable property can be an objective opinion of the courts, but the recommended approach is that it is a property determined through a subjective opinion of both the data subject and the controller. Determining a level of privacy violation or even the risk of a violation may be challenging, but to achieve trust between platforms and data subjects it is key to the future adoption of intelligent services. Trust as a key design goal has been presented as the means that the data subject can conveniently and actively participate in making processing of personal data transparent. For platforms this means that also processing made by third-parties (e.g. app developers for smartphones) must be reported through the same platform in a convenient and user friendly manner.

The thesis has argued that data protection in relation to platforms should not focus purely on anonymity, but ought to examine data protection from a more

holistic perspective, as a function of a service objective. To return and retain the individual user´s trust in digital services, while maintaining the generative mechanisms needed to build tomorrow's platforms that employs intelligent services, will require a platform privacy regulation that opens the processing silos of today. This can be achieved through the resolutions proposed to compel companies to introduce both an organisational and logical change.
The GDPR may even be strengthening the platforms with a large degree of vertical integration, as these platforms will be allowed to process personal data from each of the vertical layers, whereas others may not handle such personal data that is not directly connected with the contractual service offered. This should however not only be seen as criticism, but it may also offer the EU regulator an opportunity, a way to legally distinguish between platforms that deliver intelligent services and all other websites that may at some time handle personal data.

7.4.1. Concluding Discussion

Some may argue that the legislative process should be reactive and not anticipating in nature. The question of regulating platforms then becomes how much evidence is needed before the regulator may react. An independent source (Parse.ly 2017) summarises that Facebook and Google platforms combined currently have a direct influence over nearly 70% of where the internet traffic is directed.[61] This in addition to the personal data they store on each user. As earlier stated Google considers its data collection efforts to reach over 90% of all Internet users. A former manager of Facebook tasked with ensuring user privacy, stated that the platform maintains no responsibility in regards to third-party developers when they overuse personal data on the platform and even arguing that it is not in Facebooks interests to care about such violations (Parakilas 2017). Thus, provided privacy and perhaps most importantly consumer choice is valued in our digital society, then opening the processing silos that constitute the platform business model is required. The proposed resolutions offer a starting point for this work, and as considered earlier there are many technical details that need to be agreed upon to achieve an open data flow.

Distributed architectures and the decentralised platforms built upon these, will introduce their own set of problems that need to be analysed and solved in future research. Decentralised platforms and technology offers researchers completely new problems to investigate for the foreseeable future. Still, we take the position that centralised platforms are so effective and efficient that a new platform privacy regulation is needed to allow for new competing solutions to develop outside these platforms. The proposed shift in rationale should be on enabling data subject-

[61] Parse.ly's Network Referrer Dashboard provides insight into referral traffic to the 2500+ sites in Parse.ly's network of online media sites.

initiated open data flow. This will only be possible if companies, standards, technology, and legislation is developed in unison.

The ability for the data subject to select providers for intelligent systems is of great importance if we value our democratic rights to form our own opinions. For example, the immersive environments of virtual reality and the prescriptive power of artificial intelligence will form future generations to come. Perhaps even to the degree of replacing certain educational institutions. To achieve prescriptive artificial intelligence, for example in the form of intelligent personal assistants, the models need complete access to the user's past and present existence. If we value individualism, democracy, and a free market, then the personal data processing silos that platforms today exhibit, need to be removed. Here, it is important to understand that platforms by definition are markets that allow counterparties to trade. As earlier stated, this trade is not the problem; future markets should however be open for every market participant on equal terms. To achieve such markets, payment for any transaction needs to have a monetary value defined and not as today that insights from personal data are provided as a collateral trade. A transformation to monetary denoted payments also has an importance for society at large, for example the ability to tax these platform markets and for determining anti-competitive behaviour. At the moment taxable income from digital platforms offering "free to use" services are outside the scope of most European countries. Enabling an environment with monetary valued transaction costs offers many benefits, including opportunities for countries to collect tax based on consumption, just as in the physical society, and most importantly a cost for unnecessarily processing personal data.

User-friendly Legal Science realises the qualitative approach of design science. The aim is to develop an interpretive understanding through a holistic approach to the subject, which should describe societal reality from different perspectives. Research questions should be sufficiently narrow and answers are to be developed through the hermeneutical circle to achieve a holistic view. User-friendly Legal Science suggests an observational method in order to explore an artefact in its environment, and here the primary artefact is the GDPR. The thesis as a whole is therefore based on a descriptive part and then combined with an interpretivist part that includes qualitative problem solving and technical case studies. User-friendly Legal Science thus involves both questions that are descriptive and normative. For theories that are descriptive, the test is in their coherence with the words of the statute and with factual judicial practice, while for theories that are normative, the ultimate test lies in the justice and reasonableness of their consequences (Peczenik 2005). The objective in the thesis is to establish the notion of trust as a key design goal for future information systems handling personal data. This has been achieved by not limiting the analysis to positive law or technology, but rather by providing a holistic view of the interconnectedness of law, economics, society, and technology. The hermeneutical circle is closed by delivering a de lege ferenda resolution connected to platforms and a technological framework to industry and information system researchers.

To know that we know what we know, and to know that we do not know what we do not know, that is true knowledge.

—Nicolaus Copernicus

References

Ackoff, R. L. (1956). The development of operations research as a science. *Operations Research*, 4(3), 265-295.

Albrecht, P. (2015). EU General Data Protection Regulation State of play and 10 main issues. Accessed 31.8.2017, http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf.

Aldhouse, F. and Upton, E. (2015). What is to be done with the e-Privacy Directive? - Part 1, 30 October 2015. Accessed 22.11.2017 http://www.twobirds.com/en/news/articles/2015/global/what-is-to-be-done-with-the-e-privacy-directive-part-1

Argenton, C. and Prüfer, J., (2012). Search Engine Competition with Network Externalities, *Jnl of Competition Law & Economics* 8 (1), pp. 73-105.

Aronson, J. E., Liang, T. P., & Turban, E. (2005). *Decision support systems and intelligent systems*. Pearson Prentice-Hall.

Arp, D., Quiring, E., Wressnegger, C., & Rieck, K. (2017). Privacy threats through ultrasonic side channels on mobile devices. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P),* pp. 35-47.

Article 29 Working Party. (2007). Opinion 4/2007 on the concept of personal data.

Article 29 Working Party. (2011). Opinion 15/2011 on the definition of consent.

Article 29 Working Party. (2013). "Opinion 03/2013 on purpose limitation" (WP 203).

Article 29 Working Party. (2016). "Guidelines on the right to data portability" (WP 242)

Ausloos, J. (2012). The 'right to be forgotten'–worth remembering?. *Computer Law & Security Review*, 28(2), 143-152.

Austin, T., Manusama, B., and Brant, K.F. (2014). Virtual Personal Assistants. In *Hype Cycle for Human-Computer Interaction*. Ghubril, A.C. and Prentice, S., Gartner, Inc. G00264133. p. 12.

Begoli, E. (2012). A Short Survey on the State of the Art in Architectures and Platforms for Large Scale Data Analysis and Knowledge Discovery from Data," *Proceedings of the WICSA/ECSA 2012*, Companion Volume, ACM, pp. 177-183.

Bell, D. E., Raiffa, H., & Tversky, A. (Eds.). (1988). *Decision making: Descriptive, normative, and prescriptive interactions*. Cambridge University Press.

Big Data Working Group. (2013). Big data analytics for security intelligence. *CSA Cloud Security Alliance*, Accessed 09.09.2017 https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf.

Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law & Security Review*, Vol. 24(6), pp. 508–520.

Borgatti, S. P., Mehra, A., Brass, D. J., and Labianca, G. (2009). Network analysis in the social sciences. *Science*, 323(5916), pp. 892–895.

Bergkvist, A., Burnett, D.C., Jennings, C., Narayanan, A., Aboba, B., Brandstetter, T. (2017). WebRTC 1.0: Real-time Communication Between Browsers, *W3C*, Working Draft 22 August 2017. Accessed 22.08.2017 https://www.w3.org/TR/webrtc/.

Boyd, V. (2006). Financial privacy in the United States and the European Union: A path to transatlantic regulatory harmonization. *Berkeley J. Int'l L.*, 24, 939.

Bruegger, B. P., & Roßnagel, H. (2016). Towards a Decentralized Identity Management Ecosystem for Europe and Beyond. In *Open Identity Summit* (pp. 55-66).

Brynjolfsson, E., and McAfee, A. (2014). *The second machine age: work, progress, and prosperity in a time of brilliant technologies*. WW Norton & Company.

Bräutigam, T. (2012). Getting High on Information? The European Commission's Proposal for Renewal of the Data Protection Legislation. *JFT – Journal of the Law Society of Finland* (5/2012), pp. 415–435.

Buttarelli, G. (2015) European Data Protection Supervisor Opinion 4/2015, Towards a new digital ethics: Data, dignity and technology.

Bygrave, L. A. (2001). Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling. *Computer Law & Security Review*, 17(1), 17-24.

Carlsson, C., & Fullér, R. (1996). Fuzzy multiple criteria decision making: Recent developments. *Fuzzy sets and systems*, 78(2), 139-153.

Case 24117/08, Bernh Larsen Holding AS and Others v. Norway. European Court of Human Rights (ECtHR).

Case C-101/01, Lindqvist. European Court of Justice (ECJ).

Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Court of Justice of the European Union (CJEU).

Case C-362/14, Schrems v Data Protection Commissioner. Court of Justice of the European Union (CJEU).

Case (C-524/06) Heinz Huber v Bundesrepublik Deutschland. Court of Justice of the European Union (CJEU).

Case Murphy v. Perger, [2007] O.J. No. 5511, 67 C.P.C. (6th) 245 (S.C.J.) Canada.

Cerf, V. G., & Quaynor, N. (2014). The Internet of Everyone. *Internet Computing, IEEE*, *18*(3), pp. 96-96.

Chaffey, D. and Smith PR. (2013). *Emarketing Excellence: Planning and Optimizing your Digital Marketing 4ed.* pp. 104-106. Routledge.

Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS quarterly*, 36(4), 1165-1188.

Chen, X. W., & Lin, X. (2014). Big data deep learning: challenges and perspectives. *IEEE access*, 2, 514-525.

Cleff, E. B. (2007). Implementing the legal criteria of meaningful consent in the concept of mobile advertising. *Computer Law & Security Review*, 23(3), 262-269.

Costa, L. and Poullet, Y. (2012). Privacy and the regulation of 2012. *Computer Law & Security Review* (28), pp. 254–262.

Crane, S., Larsen, P., Brunthaler, S., & Franz, M. (2013, December). Booby trapping software. In *Proceedings of the 2013 workshop on New security paradigms workshop* (pp. 95-106). ACM.

Crary, K., and Sullivan, M. J. (2015). Peer-to-peer affine commitment using bitcoin. In *ACM SIGPLAN Notices* (Vol. 50, No. 6, pp. 479-488). ACM.

Cusumano, M. A., & Gawer, A. (2002). The elements of platform leadership. *MIT Sloan management review*, *43*(3), 51.

Danks, D., & London, A. J. (2017). Algorithmic Bias in Autonomous Systems. In *Proceedings of the 26th International Joint Conference on Artificial Intelligence* (IJCAI 2017). pp. 4691--4697.

Data Protection Commissioner - Ireland. (2017). Anonymisation and pseudonymisation. Office of the Data Protection Commissioner. Ireland. Accessed 15.08.2017 https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm.

Davenport, T. H. (2006). Competing on analytics. *Harvard business review*, *84*(1), 99-107.

Davenport, T. H. (2013). Analytics 3.0. *Harvard Business Review*, 91(12), 64-+.

De Hert, P. & Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review* (28), pp. 130–142.

Dean, J., & Ghemawat, S. (2004). MapReduce: Simplified Data Processing on Large Clusters. Appeared in *OSDI '04: 6th Symposium on Operating Systems Design and Implementation*. USENIX Association. San Francisco, CA.

Delen, D., & Demirkan, H. (2013). Data, information and analytics as services. *Decision Support Systems*, 55(1), 359-363.

De Mauro, A., Greco, M., & Grimaldi, M. (2015). What is big data? A consensual definition and a review of key research topics. In *AIP conference proceedings* (Vol. 1644, No. 1, pp. 97-104). AIP.

Dembosky, A., & Fontanella-Khan, J. (2013). US tech groups criticised for EU lobbying. *Financial Times*, 4(2013), 8.

Diakopoulos, N., and Friedler, S. (2016). How to hold algorithms accountable. *MIT Technology Review*, 17(11), 2016.

Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F., Mustafin, R., & Safina, L. (2016). Microservices: yesterday, today, and tomorrow. *arXiv preprint arXiv:1606.04036*.

Duffy, A. (2017). Google is linking secret, court-protected names - including victim IDs - to online coverage. *Ottawa Citizen*. Accessed 23.09.2017 http://ottawacitizen.com/news/local-news/google-is-linking-secret-court-protected-names-including-victim-ids-to-online-coverage.

Duffy, J. (2012). Google+, PCMag.com. Accessed 22.09.2017 http://www.pcmag.com/article2/0,2817,2389224,00.asp.

Duhigg, C. (2012). How Companies Learn Your Secrets. *The New York Times*, 16.2.2012 (Online version: http://www.nytimes.com).

Eckersley, P. (2010). How unique is your web browser?. In *Privacy Enhancing Technologies* Vol. 6205, pp. 1-18.

Ekholm, J. and Blau, B. (2014). Cognizant Computing Analysis. In *Hype Cycle for Human-Computer Interaction*. Ghubril, A.C. and Prentice, S., Gartner, Inc. G00264133. p. 16.

Eliassen, K. A., Nfa, M. S., & Sjovaag, M. (Eds.). (2013). *European telecommunications liberalisation*. Routledge.

Enkvist and Westerlund (2013). Personuppgiftsskydd – med särskild betoning på profilering, *JFT – Journal of the Law Society of Finland* (2)2013, pp. 85-113.

Enkvist, J., Westerlund, M. & Honkanen, P. (2017). Smarta avtal – en utmaning för avtalslagen? *JFT – Journal of the Law Society of Finland*, (1)2017 p.55-69.

Enkvist-Gauffin, J. (2006). *Spam–Spim–Spit. En marknadsrättslig undersökning av marknadsföring via nya kommunikationstekniker*. LLD thesis. University of Helsinki/Hanken School of Economics.

European Commission. (2015). Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy. Accessed 1.12.2015 https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud.

European Commission. (2017). Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover. Accessed 31.10.2017 http://europa.eu/rapid/press-release_IP-17-1369_en.htm.

European Parliament. (2017). European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Accessed 08.11.2017 http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2017-0051

Evans, J. R., & Lindner, C. H. (2012). Business analytics: The next frontier for decision sciences. *Decision Line*, 43(2), 4-6.

Feigenbaum, E. A., & Buchanan, B. G. (1993). DENDRAL and META-DENDRAL: Roots of knowledge systems and expert system applications. *Artificial Intelligence*, 59(1-2), 233-240.

Filippi, P., & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday, 21*(12).

Fox, G.C. (2012, October). Large Scale Data Analytics on Clouds. Proceedings of the fourth *International workshop on cloud data management*, ACM, pp. 21-23.

Gallant, S. I. (1993). *Neural network learning and expert systems*. MIT press.

Gawer, A., & Cusumano, M. A. (2008). How companies become platform leaders. *MIT Sloan management review*, 49(2), 28.

Gawer, A., & Cusumano, M. A. (2014). Industry platforms and ecosystem innovation. *Journal of Product Innovation Management*, 31(3), 417-433.

Ghazal, A., Rabl, T., Hu, M., Raab, F., Poess, M., Crolotte, A., & Jacobsen, H. A. (2013, June). BigBench: towards an industry standard benchmark for big data analytics. In *Proceedings of the 2013 ACM SIGMOD international conference on Management of data* (pp. 1197-1208). ACM.

Gomez, J., Pinnick, T., & Soltani, A. (2009). Know privacy: The current state of web privacy, data collection, and information sharing. *Berkeley, CA: UC Berkeley School of Information.*

Goodfellow, I., Shlens, J., and Szegedy, C. (2015). Explaining and harnessing adversarial examples. In *Proceedings of the 2015 International Conference on Learning Representations*.USA.

Grace, M. C., Zhou, W., Jiang, X., and Sadeghi, A-R. (2012). Unsafe exposure analysis of mobile in-app advertisements. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks (WISEC '12)*. ACM, New York, NY, USA, 101-112.

Grahn, K., Westerlund, M., & Pulkkis, G. (2017). Analytics for Network Security: A Survey and Taxonomy. In *Information Fusion for Cyber-Security Analytics* (pp. 175-193). Springer International Publishing.

Grover, V., & Lyytinen, K. (2015). New State of Play in Information Systems Research: The Push to the Edges. *MIS Quarterly*, *39*(2).

Grunes, A. P., & Stucke, M. E. (2015). No Mistake About It: The Important Role of Antitrust in the Era of Big Data. *Antitrust Source* (Apr. 2015 (4)).

Hackett, R. (2016). LinkedIn Lost 167 Million Account Credentials in Data Breach. Fortune. Accessed 22.09.2017, http://fortune.com/2016/05/18/linkedin-data-breach-email-password/.

Hagiu, A. and Altman, E.J. (2017). Finding the Platform in Your Product. *Harvard Business Review*. Issue July–August 2017, (pp.94–100).

Harrison, M. P., Beatty, S. E., Reynolds, K. E., & Noble, S. M. (2015). Why Customers Stay in Relationships: The Lock-in Factors. In *Proceedings of the 2008 Academy of Marketing Science (AMS) Annual Conference* .pp. 94-94. Springer, Cham.

Hardt, D. (2012). The OAuth 2.0 Authorization Framework. Internet Engineering Task Force (IETF). Accessed 29.10.2017 https://datatracker.ietf.org/doc/rfc6749/

Hart, H. L. A. (1961, 1994). *The concept of law*. 2nd ed., Claredon Press, Oxford.

Haucap, J., & Heimeshoff, U. (2014). Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization?. *International Economics and Economic Policy*, 11(1-2), 49-61.

Haykin, S.O. (2009). *Neural Networks and Learning Machines*, 3rd ed. Pearson Prentice Hall, USA.

Henfridsson, O., & Bygstad, B. (2013). The generative mechanisms of digital infrastructure evolution. *MIS quarterly*, 37(3).

Hickson, I. (2016). Web Storage (Second Edition): W3C Recommendation 19 April 2016. Accessed 22.08.2017 http://www.w3.org/TR/webstorage/.

Hildebrandt, M. (2009). Who is Profiling Who? Invisible Visibility, in Gutwirth, S et al. (Eds.) *Reinventing Data Protection?* Springer Netherlands, pp. 239–252.

Holmes, N. (2003). Revising the principles of technorealism [professional aspects]. *Computer*, *36*(1), 128-127.

Holton, R. (1998). Positivism and the internal point of view. *Law and Philosophy*, 17(5), 597-625.

Honkanen, P. (2017). Lohkoketjuteknologian lupaus. Arcada Working Papers, (1)2017.

HTML5. (2014). A vocabulary and associated APIs for HTML and XHTML, W3C Recommendation 28 October 2014. Accessed 22.08.2017 https://www.w3.org/TR/2014/REC-html5-20141028/.

Hu, Q., Lv, S., Shi, Z., Sun, L., & Xiao, L. (2017, June). Defense Against Advanced Persistent Threats with Expert System for Internet of Things. In *International Conference on Wireless Algorithms, Systems, and Applications* (pp. 326-337). Springer, Cham.

Huang, G. B., Chen, L., & Siew, C. K. (2006). Universal approximation using incremental constructive feedforward networks with random hidden nodes. *IEEE Trans. Neural Networks*, 17(4), 879-892.

IBM. (2010). IBM Business Analytics software for healthcare. Solution Brief. *IBM*. Accessed 14.08.2017 http://docshare04.docshare.tips/files/3848/38481003.pdf.

Javed, I. T., et al. (2017). Cross-domain identity and discovery framework for web calling services. *Annals of Telecommunications*, *72*(7-8), 459-468.

Kaisler, S., Armour, F., Espinosa, J. A., & Money, W. (2013). Big data: Issues and challenges moving forward. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 995-1004). IEEE.

Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, 32(3), 61.

Kohonen, T.: Automatic formation of topological maps of patterns in a self-organizing system. In: *Proc. 2nd Scand. Conf. on Image Analysis*, pp. 214–220, Oja, E., Simula, O. (eds.). Espoo: Suomen Hahmontunnistustutkimuksen Seura 1981.

Korolova, A. (2010). Privacy violations using microtargeted ads: A case study. In *Data Mining Workshops (ICDMW), 2010 IEEE International Conference on* (pp. 474-482). IEEE.

Krasnova, H., & Kift, P. (2012). Online privacy concerns and legal assurance: a user perspective. In *AIS SIGSEC WISP Workshop on Information Security and Privacy* pp. 1-23.

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. In *Advances in neural information processing systems* (pp. 1097-1105).

Kshetri, N. (2017). Can Blockchain Strengthen the Internet of Things?. *IT Professional*, *19*(4), 68-72.

Laney, D. (2001). 3D data management: Controlling data volume, velocity and variety. *META Group Research Note*, *6*, p. 70.

Lessig, L. (1995). The path of cyberlaw. *The Yale Law Journal*, 104(7), 1743-1755.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Lessig, L. (2000). Code is law: On liberty in cyberspace. *Harvard Magazine*, (January-February), 1-2.

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

Lewis, J. and Fowler, M. (2014). Microservices, Accessed 22.09.2017 http://martinfowler.com/articles/microservices.html.

Leyden, J. (2017). Google launches root certificate authority. The Register.

Accessed 02.09.2017 https://www.theregister.co.uk/2017/01/27/google_root_ca/.

Liberatore, M. J., & Luo, W. (2010). The analytics movement: Implications for operations research. *Interfaces*, 40(4), 313-324.

Liu, B. (2010). Sentiment analysis and subjectivity. In *Handbook of Natural Language Processing,* 2nd Ed. Taylor and Francis Group, Boca.

Lorscheid, I., & Troitzsch, K. G. (2009). How do agents learn to behave normatively? machine learning concepts for norm learning in the emil project. In *Proceedings of the sixth conference of ESSA*.

Lunden, I. (2014). Here's The 3 Reasons Europe Green-Lighted Facebook's $19B WhatsApp Deal. *Techcrunch*. Accessed 31.10.2017 https://techcrunch.com/2014/10/03/heres-europes-3-reasons-why-it-approved-the-19b-facebook-whatsapp-deal/.

Lynch, G. (2017). EU Court Ruling May Signal Problems for Data Privacy Shield. *Bloomberg Law: Privacy and Data Security*.

Lynge, E. (1995). New draft on European directive on confidential data. *BMJ: British Medical Journal*, *310*(6986), 1024.

Lyytinen, K., & Yoo, Y. (2002). Research commentary: the next wave of nomadic computing. *Information systems research*, 13(4), 377-388.

Ma, C. Y., Yau, D. K., Yip, N. K., & Rao, N. S. (2013). Privacy vulnerability of published anonymous mobility traces. *IEEE/ACM Transactions on Networking (TON)*, 21(3), 720-733.

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy. *Pew Research Center*, *21*, 2-86.

Mainelli, M. (2017). Blockchain Could Help Us Reclaim Control of Our Personal Data. Harvard Business Review – Web site. Accessed 8.11.2017 https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data.

Marsh, S.P. (1994). *Formalising trust as a computational concept*. PhD thesis, University of Stirling.

MacMillan, L. (2010). Six keys to real-time analytics: How to maximize analytics initiatives. *Business Information Review*, 27(3), 141-143.

Malone, T. W., & Bernstein, M. S. (2015). *Handbook of collective intelligence*. MIT Press.

McGrath, R. G. (2010). Business models: A discovery driven approach. *Long range planning*, 43(2), 247-261.

McKinnon, A. (2014). Sacrificing Privacy for Convenience: The Need for Stricter FTC Regulations in an Age of Smartphone Surveillance. J. Nat'l Ass'n Admin. L. Judiciary, 34, 484.

Mehta, N., Sicking J., Graff, E., Popescu, A., Orlow, J., Bell, J. (2015). Indexed Database API: W3C Recommendation 08 January 2015. Accessed 22.08.2017 http://www.w3.org/TR/IndexedDB/.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497-1516.

Mnih, V., Badia, A. P., Mirza, M., Graves, A., Lillicrap, T., Harley, T., Silver, D., & Kavukcuoglu, K. (2016). Asynchronous methods for deep reinforcement learning. In *International Conference on Machine Learning* (pp. 1928-1937).

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. The *Journal of Supercomputing*, 63(2), 561-592.

Moffatt, S. (2016). Blockchain for Identity: Access Request Management. Accessed 27.10.2017 www.theidentitycookbook.com/2016/06/blockchain-for-identity-access-request.html.

Morse, P. M., & Kimball, G. E. (1946). Methods of operations research (No. OEG-54). *Center for Naval Analyses Alexandria VA Operations Evaluation Group*. USA.

Moser, J. (2016). Consent and contract under GDPR – Prohibition of consent bundling. Datareality. Accessed 24.11.2017 https://datareality.eu/consent-contract-gdpr-bundling/.

Mossalam, H., Assael, Y. M., Roijers, D. M., & Whiteson, S. (2016). Multi-objective deep reinforcement learning. *arXiv preprint arXiv:1610.02707*.

Mäntysaari, P. (2017). *User-friendly Legal Science: A New Scientific Discipline*. Springer.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Narayanan, A., Paskov, H., Gong, N. Z., Bethencourt, J., Stefanov, E., Shin, E. C. R., & Song, D. (2012, May). On the feasibility of internet-scale author identification. In *Security and Privacy (SP)*, 2012 IEEE Symposium on (pp. 300-314). IEEE.

Neff, G., & Nagy, P. (2016). Automation, Algorithms, and Politics: Talking to Bots: Symbiotic Agency and the Case of Tay. *International Journal of Communication*, 10, 17.

Newman, L.H. (2017a). So, Uh, That Billion-Account Yahoo Breach Was Actually 3 Billion. *Wired*. Accessed 15.10.17 https://www.wired.com/story/yahoo-breach-three-billion-accounts/.

Newman, L.H. (2017b). Replacing Social Security Numbers Won't Be Easy, but It's Worth It. *Wired*. Accessed 15.10.17 https://www.wired.com/story/social-security-number-replacement/.

O'Brien, M. (2017). The company says the stolen information did not include bank accounts or payment cards information. *Inc.com/AP*. Accessed 15.10.17 https://www.inc.com/associated-press/all-3-billion-yahoo-accounts-hacked-2013.html.

Oracle. (2012). Big data analytics technology brief: Customer segmentation engines as building block. White Paper, *Oracle Corporation*. Accessed 14.08.2017 http://www.oracle.com/us/technologies/big-data/bda-customer-segmentation-engines-2045188.pdf.

Paarnio, P., Stenvall, S., Westerlund, M., and Pulkkis, G. (2015). Active Intrusion Management for Web Server Software: Case WordPress, *Tenth International Multi-Conference on Computing in the Global Information Technology (ICCGI 2015)*. IARIA.

Palmer, M. (2006) Data is the New Oil, accessed 9.7.2017 http://ana.blogs.com/maestros/2006/11/data_is_the_new/.

Parakilas, S. (2017) We Can't Trust Facebook to Regulate Itself. Opinion Nov. 19, 2017. *New York Times*. Accessed 19.11.2017 https://www.nytimes.com/2017/11/19/opinion/facebook-regulation-incentive.html.

Parent, W. (1983). Privacy, Morality and the Law. *Philosophy and Public Affairs.* Princeton, NJ, *12*(4), 269-288.

Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). *Platform revolution: How networked markets are transforming the economy--and how to make them work for you*. WW Norton & Company.

Parse.ly (2017, Dec. 10). External Referral Traffic to Parse.ly's Customers. Accessed 10.12.2017 https://www.parse.ly/resources/data-studies/referrer-dashboard/

Peczenik, A. (2005) Legal Doctrine and Legal Theory. In Scientia Juris: Legal Doctrine as Knowledge of Law and as a Source of Law, Vol 4(1). In *A Treatise of Legal Philosophy and General Jurisprudence Pattaro*, E. (eds.). Springer, Dordrecht

Perez-Botero, D., Szefer, J., & Lee, R. B. (2013, May). Characterizing hypervisor vulnerabilities in cloud computing servers. In *Proceedings of the 2013 international*

workshop on Security in cloud computing (pp. 3-10). ACM.

Pfitzmann, A., & Hansen, M. (2010). Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology. Version v0.34 Aug. 10, 2010. Accessed 1.11.2017 https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

Prandini, M., & Ramilli, M. (2012). Return-oriented programming. *IEEE Security & Privacy*, 10(6), 84-87.

Pulkkis, G., Karlsson, J., and Westerlund, M. (2018). "Blockchain-based security solutions for iot systems" in *Internet of Things A to Z: Technologies and Applications*, Hassan, Q. F. Ed. USA: John Wiley and Sons, Inc., ch. 9, pp. 255–273.

PWC (2013). Understanding a financial statement audit. Accessed 7.11.2017 http://download.pwc.com/ie/pubs/2014-pwc-ireland-understanding-financial-statement-audit.pdf

Raval, S. (2016). *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. O'Reilly Media, Inc.

Regan, P. M. (2003). Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows. *Journal of Social Issues,* Vol. 59(2), pp. 263–282.

Rochet, J. C., & Tirole, J. (2003). Platform competition in two-sided markets. *Journal of the European Economic Association*, 1(4), 990-1029.

Roemer, R., Buchanan, E., Shacham, H., & Savage, S. (2012). Return-oriented programming: Systems, languages, and applications. *ACM Transactions on Information and System Security (TISSEC)*, 15(1), 2.

Russell, A., Song, J., Archibald, J., Kruisselbrink, M. (2016). Service Workers 1: W3C Working Draft, 11 October 2016. Accessed 22.08.2017 https://www.w3.org/TR/service-workers-1/.

Råman, J. (2006). *Regulating Secure Software Development*. PhD thesis. University of Lapland, Rovaniemi.

Sandgren, C. (2000). On Empirical Legal Science. *Scandinavian Studies in Law*, vol. 40, 445-482.

Savola, R., Frühwirth, C. and Pietikäinen, A. (2012). Risk-Driven Security Metrics in Agile Software Development – An Industrial Pilot Study. *J. Universal Computer Science*, vol. 18, no. 12, pp. 1679-1702.

Schoeman, F. (1984). Privacy: philosophical dimensions. *American Philosophical Quarterly*, 21(3), 199-213.

Seipel, P. (2004) IT Law in the Framework of Legal Informatics. *Scandinavian Studies in Law*, Vol. 47, pp. 31-47.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., and Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems* (pp. 2347-2356). ACM.

Simonite, T. (2016). Tesla Tests Self-Driving Functions with Secret Updates to Its Customers' Cars. *MIT Tech. Review*. Accessed 22.09.2017, https://www.technologyreview.com/s/601567/tesla-tests-self-driving-functions-with-secret-updates-to-its-customers-cars/

Smith, A. (2014). What Internet Users Know about Technology and the Web. *Market Study, Internet, Science, and Technology*. The Pew Research Center.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 35(4), 989-1016.

SOA Manifesto, Available at, http://www.soa-manifesto.org/ last accessed on August 26, 2017.

Solove, D. J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, Vol. 126, pp. 1880–1903.

Sovilj, D., Eirola, E., Miche, Y., Björk, K. M., Nian, R., Akusok, A., & Lendasse, A. (2016). Extreme learning machine for missing data using multiple imputations. *Neurocomputing*, 174, 220-231.

Spode, E.J. (2017). The great cryptocurrency heist. Aeon. 14 February 2017. Accessed 02.09.2017 https://aeon.co/essays/trust-the-inside-story-of-the-rise-and-fall-of-ethereum.

Sprague, R. H. (1987). DSS in context. *Decision Support Systems*, 3(3), 197-202.

Spulber, D. F. and Yoo, C. S. (2014). Antitrust, the Internet, and the Economics of Networks. In *The Oxford handbook of international antitrust economics* (Vol. 1) Blair, R.D., & Sokol, D.D. (eds.). Oxford University Press, USA, pp. 380-403.

Sørensen, C., & Landau, J. S. (2015). Academic agility in digital innovation research: The case of mobile ICT publications within information systems 2000–2014. *The Journal of Strategic Information Systems*, 24(3), 158-170.

Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, 8(6), 24-31.

Tanenbaum, A. S., & Van Steen, M. (2007). *Distributed systems: principles and paradigms.* Prentice-Hall.

Taylor, J. (2012). Applying Analytics at Production Scale. In Davenport, T. (Ed.) *Enterprise Analytics: Optimize Performance, Process, and Decisions Through Big Data*, FT Press, pp. 97–110.

Thielman, S. (2016). Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian*. Accessed 22.09.2017, https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached.

Thomas, O. (2005). Understanding the term reference model in information systems research: history, literature analysis and explanation. In *International Conference on Business Process Management* (pp. 484-496). Springer, Berlin, Heidelberg.

Tuyls, K., & Parsons, S. (2007). What evolutionary game theory tells us about multiagent learning. *Artificial Intelligence*, 171(7), 406-416.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. (2012). ULD issues orders against Facebook because of mandatory real names. Accessed 20.09.2017 https://www.datenschutzzentrum.de/presse/20121217-facebook-real-names.htm.

Ullmann, M., Wieschebrink, C. and Kugler, D. (2015). Public Key Infrastructure and Crypto Agility Concept for Intelligent Transportation Systems, In *Proceedings for the Fourth International Conference on Advances in Vehicular Systems, Technologies and Applications*.

Vaidya, J., Zhu, Y. M. and Clifton, C. (2006). *Privacy Preserving Data Mining*. Springer US.

Valvåg, S.V., Johansen, D. and Kvalnes, Å. (2013). Position Paper: Elastic Processing and Storage at the Edge of the Cloud," In *Proceedings of the 2013 international workshop on hot topics in cloud services*, ACM, pp. 43-49.

van Miltenburg, E. (2016). Stereotyping and bias in the flickr30k dataset. *arXiv preprint*, arXiv:1605.06083.

van Rossum, H., Gardeniers, H., and Borking, J. (1995). *Privacy-Enhancing Technologies: The Path to Anonymity*, Vol II. TNO Physics and Electronics Laboratory. RijsWijk: Registratiekamer.

Vaquero, Á. N. (2013). Five models of legal science. *Revus: J. Const. Theory & Phil. Law, 19*, iii. p. 53-81. Translated by Bertrán, E.G. Accessed 25.7.2017 https://revus.revues.org/2449.

Verdonck, M., Gailly, F., de Cesare, S., & Poels, G. (2015). Ontology-driven conceptual modeling: A systematic literature mapping and review. *Applied Ontology*, 10(3-4), 197-227.

Vermesan, O. and Friess, P. (2011). *Internet of Things - Global Technological and Societal Trends From Smart Environments and Spaces to Green ICT*, River Publishers, Denmark.

Vigneri, L., Chandrashekar, J., Pefkianakis, I. and Heen, O. (2015). Taming the Android AppStore: Lightweight Characterization of Android Applications, *EURECOM*, Research Report RR-15-305, April 27th, 2015.

von Koskull, A. (2002) Employment Privacy Protection - Nordic Comparative Perspectives, *IT Law – Scandinavian Studies in Law*, Volume 43, p. 335-356.

Wagner, J., & Benecke, A. (2016). National Legislation within the Framework of the GDPR. *Eur. Data Prot. L. Rev.*, 2, 353.

Wahlgren, P. (2004). IT and legislative development. *Scandinavian Studies in Law*, vol. 47, 601-618.

Wei, X., Neamtiu, I., & Faloutsos, M. (2015, December). Whom Does Your Android App Talk To?. In *2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, 2015, pp. 1-6.

Westerlund, M. and Enkvist, J. (2013). Profiling Web Users – In light of the proposed EU Data Protection Regulation, *Retfaerd - Nordic Journal of Law and Justice*, Vol. 36, Nr 4/143, pp. 46-62.

Westerlund, M. and Enkvist, J. (2016). Platform privacy: the missing piece of data protection legislation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7(1)2016, pp. 2-17.

Westerlund, M. Hedlund, U., Pulkkis, G. & Björk, K-M. (2014). A Generalized Scalable Software Architecture for Analyzing Temporally Structured Big Data in the Cloud. *New Perspectives in Information Systems and Technologies*, Volume, 559, Springer.

White, A. (2016). Facebook Accused of Misleading EU in WhatsApp Takeover Probe. *Bloomberg*. Accessed 31.10.2017 https://www.bloomberg.com/news/articles/2016-12-20/facebook-gets-eu-antitrust-complaint-over-whatsapp-takeover-bid

Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*. Springer.

Wondracek, G., Holz, T., Kirda, E., & Kruegel, C. (2010, May). A practical attack to de-anonymize social network users. In *2010 IEEE Symposium on Security and Privacy (SP)*, pp. 223-238. IEEE.

Wong, R. (2007). Data Protection Online: Alternative Approaches to Sensitive Data?. *Journal of International Commercial Law and Technology*, Vol. 2(1), pp. 9–16.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access*, *5*, 14757-14767.

Xiang, J., Westerlund, M., Sovilj, D., and Pulkkis, G. (2014). Using Extreme Learning Machine for Intrusion Detection in a Big Data Environment, *7th ACM Workshop on Artificial Intelligence and Security (AISec14) collocated with 21st ACM Conference on Computer and Communications (CCS14).*

Yoo, Y. (2013). The tables have turned: How can the information systems field contribute to technology and innovation management research?. *Journal of the Association for Information Systems*, 14(5), 227.

Zittrain, J. L. (2006). The generative internet. *Harvard Law Review*, 119(7), 1974-2040.

Öman, S. (2004) Implementing Data Protection in Law, *IT Law – Scandinavian Studies in Law*, Volume 47, pp. 389–403.

Magnus Westerlund

A Study of EU Data Protection Regulation and Appropriate Security for Digital Services and Platforms

This doctoral thesis deals with and interprets the European Data Protection Regulation. The purpose of the dissertation is to establish the concept of trust as an important design goal for information systems that handle personal data. The interpretation is linked to the areas of analytics, security and privacy issues in the development of intelligent services. The centralized platform model is identified as a challenge for the data protection regulation in realising an open Internet.

I föreliggande doktorsavhandling behandlas och tolkas den Europeiska dataskyddsregleringen. Syftet med avhandlingen är att etablera begreppet förtroende som ett viktigt designmål för informationssystem som hanterar personuppgifter. Tolkningen kopplas till områdena analytik, säkerhet och integritetsfrågor för utveckling av intelligenta tjänster. Den centraliserade plattformsmodellen identifieras som en utmaning för dataskyddsregleringen i förverkligandet av visionen om ett öppet Internet.

ISBN 978-952-12-3693-8