Platform Privacy: The Missing Piece of Data Protection Legislation

by **Magnus Westerlund and Joachim Enkvist***

Abstract: After years of deliberation, the EU commission sped up the reform process of a common EU digital policy considerably in 2015 by launching the EU digital single market strategy. In particular, two core initiatives of the strategy were agreed upon: General Data Protection Regulation and the Network and Information Security (NIS) Directive law texts. A new initiative was additionally launched addressing the role of online platforms. This paper focuses on the platform privacy rationale behind the data protection legislation, primarily based on the proposal for a new EU wide General Data Protection Regulation. We analyse the legislation rationale from an Information System perspective to understand the role user data plays in creating platforms that we identify as "processing silos". Generative digital infrastructure theories are used to explain the innovative mechanisms that are thought to govern the notion of digitalization and successful business models that are affected by digitalization. We foresee continued judicial data protection challenges with the now proposed Regulation as the adoption of the "Internet of Things" continues. The findings of this paper illustrate that many of the existing issues can be addressed through legislation from a platform perspective. We conclude by proposing three modifications to the governing rationale, which would not only improve platform privacy for the data subject, but also entrepreneurial efforts in developing intelligent service platforms. The first modification is aimed at improving service differentiation on platforms by lessening the ability of incumbent global actors to lock-in the user base to their service/platform. The second modification posits limiting the current unwanted tracking ability of syndicates, by separation of authentication and data store services from any processing entity. Thirdly, we propose a change in terms of how security and data protection policies are reviewed, suggesting a third party auditing procedure.

Keywords: Platform Privacy; Data Protection; GDPR; Data Storage Solutions; Internet of Things

Recommended citation: Magnus Westerlund and Joachim Enkvist, Platform Privacy: The Missing Piece of Data Protection Legislation, 7 (2016) JIPITEC 2 para 1.

A. Introduction

1 During the last twenty years, the world has gone through a technology era often referred to as the Internet age. This has led to a tremendous change in how individuals and businesses function in daily life. Yet, across the world, privacy laws which govern the operational modus for companies providing services to consumers, may have been devised during a time when the Internet was predominantly used in research and academia. It can be argued that the Internet was initially designed without security or privacy in mind, but rather as a method for allowing countless data packets and 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 as, for example, today the data packet delivery time over large distances is to a large extent limited by physical laws and not by technological constraints. However, the impossible task of foreseeing the impact of the Internet on our social constructs, has to a large degree directed subsequent academic research in the field towards trying to solve issues of security and privacy that were omitted from the original standards. These are considerations that the initial Internet communication protocol did not address. One example is that the email communication protocol does not include an encryption policy, and as a consequence email traffic between two organisations is mostly transferred in a plain text format. Arguably,

the majority of research in the area of security and privacy is based on the assumption that anonymity in its various forms is achievable and desired.

2 The European Data Protection Directive[1] (95/46/EC) adopted in 1995 and subsequently enacted in national legislation in the separate member states, was based on the premise of the right to respect one's "private and family life, his home and his correspondence" as defined by the European Convention on Human Rights[2] (Article 8, CETS No.: 005, 1950). The subsequent point in Article 8 states: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.". In the context of the business-consumer relationship, the Data Protection Directive has consequently been interpreted that information pertaining to identifying a physical individual can only be stored and processed with the consent of the data subject. Data processing should also be proportionate in relation to the legitimate purpose pursued. The proportionality measure refers to what the minimum extent is for delivering the expected service to the data subject.[3]

3 Considering that the most dominant Internet-related service providers are often non-EU based companies (mostly US companies) and that countries such as the US have no encompassing data protection law, the enforcement of EU law for the benefit of its citizens and companies has been challenging. A recent example of such a dispute was a call from the EU Parliament to "unbundle search engines from other commercial services".[4] This stems from a fear of anti-competitive practices related to a search engine provider that has well over a 90% market share in many European member states. This can be considered a realization on behalf of the EU authorities that the data of European consumers have aided in creating a situation where the search engine provider can "[commercialise] secondary exploitation of obtained information". This has an implication on the competitiveness of other companies such as EU start-ups, which then may have a competitive disadvantage compared to the incumbent US provider with access to user data on a massive scale. The EU Parliament's statement is focused on a search provider, but it uses a language that is certainly generalizable in its relevance to other areas as well, such as social networks. As "all internet traffic should be treated equally, without discrimination, restriction or interference" and "to prevent any abuse in the marketing of interlinked services by operators". Since the US have adopted what is often referred to as a sectorial approach legislation,[5] as well as a lack of laws governing data protection particularly for search engines, this can be seen as contributing to a potential abuse of a dominant market position. The balance between fostering a positive self-enforcing environment for innovation within Information Technology enabled sectors and difficulty regarding preserving the rights of a consumer. Whilst the US believes in self-regulation by the companies, the EU has taken the opposite view and enacted what can be viewed as strong consumer protection laws. In an effort to modernize and unify data protection laws for all conditions involving a natural person in the Union, an EU Commission proposal was given for a new General Data Protection Regulation (GDPR or Regulation). We hereafter refer to the preliminary consolidated Regulation proposal text (also referred to as the outcome of the inter-institutional negotiations) on the protection of individuals with regard to the processing of personal data and on the free movement of such data (ST 5455/2016).[6]

4 Today the Internet has become a global platform for commerce and communication. It is predictable that within the coming decades this will extend to include many other areas as well, e.g. personal healthcare and home automation. These new areas will introduce a myriad of highly sensitive information sources; information that must be processed and also often stored for an indefinite and sometimes infinite period of time in order to be able to digitalize these areas. By embedding information-sharing electronics into everyday physical objects, we will create a "global cyberphysical infrastructure".[7] The term often used for describing this future Internet

1 European Commission (28 January 2015). Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market. Accessed 18.10.2015: http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm.

2 European Convention on Human Rights (1950). CETS No.: 005, Accessed 18.10.2015: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=17/02/2015&CL=ENG.

3 CAHDATA (2014) RAP03Abr, AD HOC COMMITTEE ON DATA PROTECTION. Accessed 17.2.2015: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CAHDATA-RAP03Abr_En.pdf.

4 European Parliament, MEPs zero in on Internet search companies and clouds, REF. : 20141125IPR80501, 2014. Accessed 17.2.2015: http://www.europarl.europa.eu/news/en/news-room/content/20141125IPR80501/.

5 Corbet, R. (2013). "EU v US data protection - exploring the similarities." Privacy & Data Protection, 13(6), pp. 3-4.

6 ST 5455 2016 INIT - 2012/011 (OLP), Proposal for an EU General Data Protection Regulation (2016). Accessed 02.02.2016: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1454437448923&uri=CONSIL:ST_5455_2016_INIT.

7 Miorandi, Sicari, De Pellegrini and Chlamtac (2012). Internet of things: Vision, applications and research challenges, *Ad Hoc Network*.

vision is the "Internet of Things" (IoT) and is based on standardized communication protocols and merging computer networks into a "common global IT platform of seamless networks and networked 'Smart things/objects'".[8] From the perspective of service innovation, by utilizing the Internet of Things technology, the current data protection Directive is problematic. The proportionality notion that a minimum of data should be stored for as short a time as possible, can be considered limiting for the innovation process. Unfortunately, this applies to the proposed Regulation as well, which if approved, will likely limit innovation in Europe further. The progress of technology is going in the opposite direction, i.e. to store and process as much personal data as possible and deliver services based on insights gained. In contrast to the original intention of the Regulation,[9] we anticipate that the Regulation will not open up the complete domination some incumbent global companies currently experience in regards to European consumer data. This consumer data is often said to be the commodity of the future, and is compared to the importance of oil in today's economy. Some economist may argue that there is no monopoly on data, only sector silos that limit others' access to the specific data. They are correct in that no single private organisation or platform has a monopoly on personal data. However, from a mathematical and technical perspective it means data on roughly 340M people, given that for example, a search engine platform reaches a sample size of 90% of an estimated 75% of the EU-28 population of 508M that uses the Internet once a week. From the field of big data analysis, we know that it is common that user data is incomplete, but the models can still predict with a high degree of certainty a given outcome, provided we have a population sample large enough to train on. Such an incomplete training set can be compared to a monopoly on data in the sense that this monopoly data set would just as likely be incomplete, because our physical life is not yet digitalized to the degree that every action or behaviour we make is recorded. We will however use the term "processing silo" further on to describe the ability of incumbent digital platform providers with a large market share in a certain segment to close off the market to competitors. We find that solving the issue of "processing silos" should be at the core of a future Regulation in order to restore consumers' trust in digital services. The fact that the proposal will not accomplish this - although it was widely hoped it would - should not be seen as an obstacle for ratifying the currently proposed Regulation. The Regulation is an improvement for the digital service innovation landscape in Europe when compared to the Directive. A harmonization among member states in line with the single digital market strategy is greatly needed.

5 The main focus of this paper is on the data subject's privacy. However, since the angle of study is platform privacy issues, the focus becomes intertwined with competitive behaviour in the market, considering that the ability to choose among offerings in itself can be an enhancement of privacy. Based on the proposed Regulation and current practices, this paper examines a way forward for data protection legislation that considers both the interests of individuals (data protection) and entrepreneurs (by improving competitiveness) for bringing data science based innovation back to Europe. Following the introduction, we continue by deliberating the rationale behind the data protection legislation. In the subsequent section, we highlight the challenges in common practices through examples, which indicate that platform discrimination of privacy-aware consumers is an issue in today's environment. One important finding is that consumers are currently being educated from a young age by the mobile industry in particular, to be indifferent concerning issues of privacy. The penultimate section analyses and discusses the legislation rationale in regards to how it should be modified towards looking at consumer data as a currency. A currency that belongs to the data subject and that can be loaned or sold to a service provider for a fee, but not co-owned by the service provider - this obscurity creates a legal conundrum. We emphasise how to increase competition by opening up the platforms through unravelling the "processing silos" and introducing data subject controlled "data stores". The section also formulates three core modifications to the rationale. The first is aimed at improving service differentiation on platforms by lessening the ability of incumbent global actors to lock-in the user base to their service/platform. The second modification regards limiting the current unwanted tracking ability of syndicates by separation of authentication and data store services from any processing entity. Thirdly, we propose a change in terms of how security and data protection policies are reviewed. The final section concludes our findings and recommendations.

B. Current Legal Foundation Rationale

6 At the time of writing, issues of data protection are regulated in the Data Protection Directive (95/46/EC) adopted in 1995. The directive has led to diverse

8 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, p. 10.

9 See former EU Commissar Vivian Reading's press release (SPEECH/2012/26) on transparency and data portability. Accessed 18.10.2015: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm.

legislation in the separate EU member states. The aim of the proposed General Data Protection Regulation is to eliminate this diversification among member states. A further rationale is to improve the clarity and coherence of personal data protection by strengthening individual rights and reducing administrative formalities for companies. The proposed regulation is very comprehensive, and the intention of this article is to focus on only some legal foundations in the proposal that are relevant for our discussion. A noteworthy fact is that many EU member states have, in addition to the Directive (DPD), implemented sectorial data protection legislation, e.g. within health care.

7 Writing legislation for an area under intense development has not been straightforward, and there has been a lot of criticism against the proposal. Not surprisingly one of the most critical voices has been from the business sector. Some business representatives fear that implementation of the Regulation will be expensive and harm digital service development.[10] There has even been criticism from within academia and fears that it could have negative legal consequences on research involving personal data.[11] There has however also been opposing opinions stating that the regulation will lead to better business continuity.[12] Today's digital economy is based on data, which means that personal data has become a significant economic factor,[13] and the proposed regulation will boost the digital economy.[14] The economic value of personal data has been growing rapidly, and there are estimations that the value of European citizens' personal data will grow to nearly €1 trillion annually by 2020. According to the European Commission, the proposed Regulation should offer great business opportunities, and privacy-friendly European companies ought to have a competitive advantage.[15]

8 A characteristic feature of data protection is that it is closely linked to issues of human rights granted in the EU Charter of Fundamental Rights (in particular articles 7 and 8). This was also stressed in the case Google Spain SL v Agencia Espanola de Proteccion de Datos (C-131/12), where the CJEU16 held that the data subject's fundamental rights under Articles 7 and 8 of the Charter will as a rule override the interests of the public (i.e. other Internet users) in finding information on said subject, as well as Google's economic interest. [17] One key foundation of the draft Regulation is Privacy by Design (PbD; article 23 in the proposal). The controller shall ensure that only those personal data are processed which are necessary for a specific service. Referring to PbD, privacy must be taken into consideration in the beginning of a new development project and privacy must be implemented by default in new technologies.[18] When the privacy matters are considered early in the design stage, it is considered easier to produce privacy-friendly systems.[19] Former Canadian Information and Privacy Commissioner, Cavoukian, has drawn up seven foundational principles related to PbD.[20]

9 Another key principle in the draft Regulation is to empower the data subject. Personal data may not be collected and processed without consent from the data subject. According to Recital 25 of the draft Regulation, silence or inactivity do not constitute consent. Consent shall be freely given, which means that there shall be no constraint or pressure on the person giving his or her consent.[21] The requirement of consent does not mean that the consent has to be

10 Schutte, S. (2014). New Data Protection Regulation could harm UK SMEs, Accessed 18.10.2015: http://realbusiness.co.uk/article/28580-new-data-protection-regulation-could-harm-uk-smes.

11 Myklebust, J. P. (2014). Will data protection legislation harm science?, Accessed 18.10.2015: http://www.universityworldnews.com/article.php?story=20140501112331485.

12 Ashford, W. (2015). EU data protection regulation will drive privacy by design, says Kuppinger-Cole; Accessed 18.10.2015: http://www.computerweekly.com/news/4500245095/EU-data-protection-regulation-will-drive-privacy-by-design-says-KuppingerCole.

13 Sahin, A. (2014). "New EU data protection laws: European Parliament proposes restrictive data protection laws in Europe." Computer and Telecommunications Law Review, 20(2), pp. 63-65.

14 Grac-Aubert, V. (2015). "A love and hate relationship? Recent developments in data protection and competition law." European Competition Law Review, 36(5), pp. 224-231.

15 European Commission, loc.cit.

16 CJEU (2014). Google Spain SL. Google Inc. v Agencia Espanola de Protección de Datos, Mario Costeja González, Case C-131/12, Decision of May 13, 2014.

17 Crowther, H. (2014). "Remember to forget me: the recent ruling in Google v AEPD and Costeja." Computer and Telecommunications Law Review, 20(6), pp. 163-165.

18 Salgado, M. (2013). "PIAs and privacy by design - using them to your advantage." Privacy & Data Protection, 13(8), pp. 3-5.; Walker, K. (2012). "Cookies and using data on the move." Computer and Telecommunications Law Review, 18(6), pp. 172-174.Vermesan et al. 2013, Internet of Things Strategic Research and Innovation Agenda, in *Internet of Things - Global Technological and Societal Trends.* River Publishers. Aalborg. Denmark.

19 Brown, I., Korff, D. (2010). Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments. Final report. EC, Directorate-General Justice, Freedom and Security, Contract Nr: JLS/2008/C4/011 – 30-CE-0219363/00-28.

20 For more detailed information, see: https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.

21 Solove, D. J. (2013). "Introduction: Privacy Self-Management and the Consent Dilemma". Harvard Law Review, Vol. 126, pp. 1880–1903.; Cleff, E. B. 2007. "Mobile advertising regulation. Implementing the legal criteria of meaningful consent in the concept of mobile advertising." *Computer Law & Security Review* (23), pp. 262–269.

given in written form.[22] It is possible to give explicit consent e.g. by ticking a box on a website.[23]

10 The draft Regulation outlines data portability. According to Article 18, the data subject has a right to obtain a copy of data undergoing processing in an electronic and structured format from the controller. The initial proposal defines the right to transmit all information provided by the data subject and retained by an automated processing system to another party. *Another party* is not clearly defined, but can be the data subject's own device. The controller shall not be entitled to hamper the transmission of user-submitted data. Article 18 also suggests that the data subject does not have the right to any processed artefact that has been a result of profiling. It is unclear if the controller, if requested, must delete a processed artefact such as a profile or any refined data that has been altered from its original form.

C. Platform Challenges with Proposed Legislation and Current Practices

11 In this section we will analyse data protection regulation 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 rather an analysis of how the Regulation could increase competition in the market, as a guarantee for better privacy. To achieve this, we will first briefly review the current literature on digital platforms and then analyse how the Regulation deals with current practices linked to the platform.

12 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 frequently used as an example of such an advanced ecosystem. A digital ecosystem is often described in terms of its natural counterpart, were adaptiveness, competition and sustainability define the success of the ecosystem. Lyytinen and Yoo 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 can often can be described as a platform for multi-sided markets.[24] Gawer and Cusumano[25] argued that creating either a platform or service is a strategic decision. A service is, in their judgement, an early version of a platform, a standalone product, or a service that can also exist upon a platform. To become a platform, they consider that the service must satisfy two prerequisite conditions: performing at least one essential function that can be described as a "system of use", and it should be easy to connect to or to build upon to expand the system of use.

13 Zittrain[26] explained the changes the Internet brought on digital infrastructures as generativity. In their research, Henfridsson and Bygstad[27] 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 re-combinations 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. Today we see that scalable information system architectures are often designed on the principle of microservices.[28] A microservice is a specialized self-contained software system that communicates through lightweight mechanisms and with a bare minimum of centralized management of these types of 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) 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 disappears when the service is designed as a microservice. A microservice architecture can be seen as a distributed enabler

22 Lynge, E. (1995). "New draft on European directive on confidential data". BMJ, Vol. 310, p. 1024.

23 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.

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

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

26 Zittrain, J. (2006). The Generative Internet, 119 Harvard Law Review Volume 199:1974.

27 Henfridsson, O., & Bygstad, B. (2013). The generative mechanisms of digital infrastructure evolution. MIS quarterly, 37(3), 907-931.

28 Lewis, J. and Fowler, M. (2014). Microservices, Accessed 4.10.2015: http://martinfowler.com/articles/microservices.html.

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 forms, e.g. as a market for distributing games and applications between consumers and third-parties. A second important insight from the generative mechanisms is the role adaption plays in the availability of user data. As we will discuss later on in section D, the possibility of being able to process user data is at the core of the success of a digital platform, but it is also at the core of regulating platform privacy.

14 In a recent Gartner report, Ekholm and Blau[29] analyse the next step in the evolution of the personal cloud connected to the vision of the Internet of Things. They use the term Cognizant computing for describing 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.[30] defines 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". Gartner estimates 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 data sets. The vision set forth is that it will be in the data subject's best interest to open up as much of their lives as possible to the companies that offer these services, in order to benefit from them.

15 Henfridsson and Bygstad[31] 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 for the rational governing of the legal texts as well? Instead of examining data protection as individual forces that exert pressure as suggested by Lessig,[32] we ought to examine this as a function of a service objective. 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?

16 One can put forth the argument that the Regulation should not deal with platform issues, but rather focus on the data subject. The proposed Regulation has already grown approximately ten-fold 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 and network security regulation. In September 2015, the EU commission consequently launched a public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy.[33] The consultation was motivated by a need to gain a better understanding of online platforms and the necessity for further regulation. In particular, the consultation focused on illegal content on platforms, such as copyright issues, but it also highlights transparency issues. Here we will continue examining the privacy rights issues that are closely linked to data protection, which we find is not elaborated in the current data protection Regulation proposal. 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. Current platform owners, have had very little incentive to develop platform privacy since the relationships with the consumer are mostly governed by unilateral contracts, i.e. provider defined.

I. Unreasonable Expectations

17 The Regulation demands that each interaction between the data subject and controller involving data identifying the subject begins with a consent to process this data. Common current practices, as later described in regards to consent contracts often strive to outmanoeuvre or simply void earlier described legislation. Maintaining a limited number of these often highly complex consent contracts should

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

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

31 Henfridsson, O., and Bygstad, B. (2013). The generative mechanisms of digital infrastructure evolution. MIS quarterly, 37(3), 907-931.

32 Lessig, L. (1999) *Code and other laws of cyberspace*, Basic Books, New York; Lessig, L. (2006) *Code Version 2.0*, Basic Books, New York; Lessig, L. (1995). The path of cyberlaw. *The Yale Law Journal*, 104(7), 1743-1755.

33 See https://ec.europa.eu/digital-agenda/en/consultations for further details. Accessed 10.02.2016.

to some degree be possible for the data subject, e.g. office tools, email, search, mobile operating system/platform, and social network. However, exceeding a certain number of these contracts will make it implausible for the average data subject to remember what he has given consent to and to whom. For example, as is the case currently, each application installed on a smartphone or service on the Internet is required to maintain their separate contracts. When sharing information, over time it will become unmanageable for the individual to control his digital presence. 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 legislation sets unreasonable expectations on the data subject. A more appropriate solution would be to impose an obligation on the controller, particularly in relation to a platform, to periodically submit information to the subject regarding what data has been collected, how data has been processed, the result of the processing, and to whom data has been shared. As an example, a mobile platform controller is the collector of the original data subject who consented to use a platform which involves the processing of personal data. The platform controller should 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 apps for accessing platform APIs, e.g. 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 obtain 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 is collected and used in extension of the platform.

18 The Regulation delegates a similarly unreasonable expectation upon supervisory authorities. Their duties include 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. As it is currently proposed, the supervisory authorities of the member states will not have resources to perform this task adequately. Certifying a platform, e.g. a mobile operating system, will require in-depth technical and considerable monetary resources to perform 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.

II. Discriminative practices Against Privacy-Aware Users

19 The business world is facing a challenge regarding the adoption of 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. Balancing the right to privacy for the individual consumer is equally demanding given this new demand and ability to process any existing data. Many of the social networking and media companies (e.g. Facebook and Twitter) and search engine companies (e.g. Google and Yahoo) employ a revenue model primarily based on delivering personalized advertisement on-site.[34] By using their service, a consumer (data subject) agrees to be shown advertisement as part of the service experience. Lately, however, many of the well-established service providers have started offering consumers the possibility to opt out of personalized advertisement. This is a development that has arisen from the data subject's right to not be subjected to automated processing that could lead to legal issues or significantly affect the data subject (art. 15 Directive). Those within the industry have argued against such a development, citing that advertisement value increases with targeted advertisement, and thus these funds 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. Therefore, companies also have a direct business interest in learning as much as possible about the data subject, which again conflicts with the legal view in the proposed 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".[35]

20 The definition of personal data in the proposed Regulation limits its applicability to physically identifiable data subjects. The lack of protection for virtual identities was raised in Westerlund and

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

35 Albrecht, P. (2015). EU General Data Protection Regulation State of play and 10 main issues. Accessed 3.3.2015: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf.

Enkvist,[36] who examined an online forum that tracks users without asking for or storing any information referring to identification of a natural person. This "example demonstrates how it is possible for a service provider to profile users without the possibility to identify the physical identity of the user." Data that has undergone pseudonymisation, which could still be attributed to a natural person by the use of additional information should be considered as information on an identifiable natural person. This protection does not apply to virtual identities. As the natural person's identity can be irrelevant for profiling with the intention of e.g. direct marketing purposes, the protection for virtual identities[37] (also referred to as pseudonyms) hence fall outside the scope of the proposed Regulation, as the Regulation only applies to data concerning an identified or identifiable natural person.

21 We continue this section by examining some current industry practices that we find challenging for the proposed 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 to grant the controller rights to user data for these services will effectively mean a refusal of service by the controller.

1. The Right to Use Pseudonyms

22 Common practice in the design of current platforms, e.g. smartphone operating systems, is to oblige 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. 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, 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. Thus, we pose the question of 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 more valuable. 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 that, the user has 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 to keep the community safer, by reducing malicious activity and improving methods for detecting such activity.

23 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. 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.[38]

2. The Right to Use a Service Without Having to Disclose Information Irrelevant for Said Service

24 The development of smartphone ecosystems with an abundance of context-aware apps have led to what can be seen as excessive collection of user data. The argument that every single mobile app provider needs access to the data subject's personal information (e.g. call logs, photos, and location) in order to use a service is in many cases too excessive and uncontrolled. Several studies have shown that users of these devices are often unaware of how much data the apps gather, but also dislike the fact when told.[39] 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".[40] In a recent examination of the

36 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.

37 Virtual identities are often used in addition to web forums, in games and virtual reality worlds.

38 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2015). ULD issues orders against Facebook because of mandatory real names. Accessed 18.10.2015: https://www.datenschutzzentrum.de/presse/20121217-facebook-real-names.htm.

39 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, CHI 2014, April 26 - May 01 2014, Toronto, ON, Canada.

40 Madden, M. Cortesi, S., Gasser, U., Lenhart, A., and Duggan, M. (2014). Parents, Teens, and Online Privacy, *Pew Research*

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 communication with sites previously associated with malware activity".[41] In their experiment they 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. The issue of mass data collection has become a part of everyday life for most smartphone and web users.[42] Grace et al.[43] 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 the purpose of 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 oversight. However, it is evident that people still 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".[44]

25 The interesting question from a legislation point of view is perhaps not to ask why people continue using these platforms or services despite the unfavourable the privacy violations, but rather how they can be given an option of determining what is 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, e.g. teaching children that if you care about your own privacy you cannot play many popular games or use apps, can be considered a discriminatory message that we strongly wish 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 conflicts with both the current Directive and proposed Regulation.

3. Privacy Policy as a Lock-In Mechanism

26 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.[45] Through a longitudinal study they observed that there has been little progress in raising 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 of service. Facebook 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 users' information between their other services such as Facebook Payments, Instagram, and WhatsApp in accordance with their respective terms. Thus a situation arises where users become so intertwined and dependent on said company, that they can arguably be considered as "locked-in". Harrison et al.[47] 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 alternative social network sites that rival the likes of Facebook. However, Facebook has become more than a social network. Today we can consider Facebook to be "the global communication platform company", often superseding national telecom carriers in voice, text, video, images, and directory services. This is in addition to their original service of users receiving notifications when friends update their profiles.

27 The issue we seek to highlight in this discussion is

Center's Internet & American Life Project, NOVEMBER 14, 2012.

41 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.

42 Ibid.

43 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, pp. 101-112.

44 Shklovski et al. loc. cit.

45 Pew Research Center (November, 2014). "What Internet Users Know About Technology and the Web".

46 Facebook Terms of Service as of 30.1.2015, Accessed 30.12.2015, https://www.facebook.com/terms.

47 Harrison, M. P., Beatty S. E., Reynolds K. E., and 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. Springer International Publishing, pp. 94-94.

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.[48] There are arguably other social network companies than Facebook, such as LinkedIn, but they are currently competing within different segments of the market.[49] 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 case of Google+, it is worth mentioning that Google began with a massive persistently signed-in user base from both its email service as well as the 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[50] 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. The authors find that this efficiency leads to an unambiguity in how market concentration affects consumer welfare.

28 Spulberg and Yoo[51] 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 seem to fail to recognize 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 silo's" are maintained. The lock-in factor at play in today's platforms mostly relate to access to user data[52] 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 advantageous by many, including media journalists.[53] 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 the desired critical mass was not achieved.

29 Many of the EU member states have positive 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, was divided by member state and not by region. The member states bound the interested telecommunication operators to adopt the 2nd Generation GSM standard through a competitive tender.[54] The change introduced the consumer to a choice of network operator, which for the first time could be based on personal preferences. Eventually even allowing the consumer the option of transferring the phone number between operators in some countries such as Finland,. This option was important, because it removed the last lock-in mechanism available to operators, to "force" consumers to stay with them. This indicates the regulators power to change market dynamics on its own accord for the benefit of the consumer. The regulatory environment improved conditions for European companies by growing the market size, but also created an enriched roaming experience for European citizens. In comparison to the social networks of today, the alternative for a non-regulated mobile telecommunication infrastructure would have been that each operator would develop their own technology that would have been incompatible with 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. Although perhaps not a failure of markets from a business point of view, it would be a drastically inferior experience from a consumer point of view.

48 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), pp. 49-61; Argenton, C. and Prüfer, J., (2012). Search Engine Competition with Network Externalities, *Jnl of Competition Law & Economics* 8 (1), pp. 73-105.

49 Facebook is estimated, by Statistica 2015, to have 1.49bn global users, whereas the total number of social network users worldwide is estimated to be 1.79bn. Accessed 25.10.2015, http://www.statista.com/topics/1164/social-networks.

50 Haucap, J., & Heimeshoff, U., loc.cit.

51 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.

52 We define user data to include describing, behavioural, created and generated data.

53 Duffy, J. (2012). Google+, PCMag.com. Accessed 30.12.2015, http://www.pcmag.com/article2/0,2817,2389224,00.asp.

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

III. A Challenging Example of Future Internet of Things Enabled Services

30 So far in this section we have examined present practices and relevant legislation. In the following part we want to illustrate what can be expected from the digital services of tomorrow. The intention is to provide the reader with a technological vision, serving as a guidance and motivation for the final discussion advocating a proposal for change.

31 During recent years we have seen the introduction of the first Internet of Things enabled devices. Among the first such products launched were personal health-monitoring devices. These were first made exclusive for various fitness enthusiasts, but have since been introduced as mass-market products. These are the type of products that can continually monitor a user's activity, location and certain bodily functions such as heart rate. An example of an advanced intended use case is to be able to remotely monitor individuals, such as elderly people in their own home. 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 falls ill. This example shows how sensitive the information gathered can be and provides a glimpse into where technological progress is heading. 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 development of service quality. Here we are referring to, in addition to previously mentioned data types, behaviour, usage, the individual's social network and their corresponding data. The 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 smartphone, where data is cached within a certain application. It is hoped that user data is 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. This example would clearly fall inside the scope of both the Directive and the Regulation, hence requiring a consensual agreement by the data subject and controller.

32 The example highlights the positive application and progressive use of data collection and processing. However, from a legal standpoint, the intention of the Regulation states that data should be collected, processed and stored in a data minimising way. On the other hand, the Regulation does not give the data subject the right to review the security in the data flow for the platform/service. As data subjects we are simply forced to trust that the controller collects data in a minimalistic way, processes data only with the data subject's best interests in mind, stores data securely, always promptly notifies us when data is shared or breached and, if and when the subject wants to close the account, expect that the provider actually deletes all data in a non-retrievable fashion. This is the primary reason why we consider the rationale behind the Regulation to be antiquated and why we call for an increased focus on platform privacy.

D. Discussion

33 User generated data has arguably become the currency of the virtual world. The more complete and timely data we have about an individual, the more it is worth to a service 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 or uniqueness. Also 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 monetize upon these earlier findings. The difficulty in setting the price also led Google to create an auction market, AdWords,[55] 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. Economic research into platforms may have yet to conclude how to value data in relation to a platform. Stucke and Grunes[56] highlighted for antitrust cases the problematic relationship of free services which are paid for by user data, where user data has no determined value. Collected user data has a value determined by any future service that can be sold to the same consumer. Therefore, it can be argued that existing user data should always be considered of value, even if left unprocessed. Stucke and Grunes probe the question of why would companies 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 bear at least the cost of the research

55 See http://www.google.com/adwords/ for further details. Accessed 10.02.2016.

56 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)).

and development that has gone into implementing said platform. Perhaps, more importantly, 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. Acknowledging that all personal data has a monetary value, although indeterminable in a generalized way, should also improve the ability of regulatory authorities to consider platform privacy in anti-competitive terms.

34 In general, privacy is of immense importance in our digital society, but particularly so in a world where we are striving to create intelligent services that can advise us humans what to do. Still consumers are saying that privacy issues are becoming a greater challenge than before and that a growing number of consumers (45%) no longer trust the companies or platforms behind some of today's digital services with their personal data.[57] Therefore, it should be highlighted that the proposed 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 should also offer 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, image, and other special categories of sensitive data) that occurs in the consumer's environment. It should then become evident that these services will need the trust of the consumer. The more encompassing data that is being processed regarding the data subject, the greater the importance of privacy and consumer choice among platform services become.

35 Early influencers on the design of privacy preserving information systems, defined the task to accomplish as "The Path to Anonymity".[58] We also find that the current EU rationale for data protection is based on the premise that anonymity is plausible and desired. The Human Rights Convention Article 8 has been interpreted as equivalent to the right for anonymity for a natural person. The design rationale presented by van Rossum, Gardeniers and Borking[59] explores a number of potential techniques regarding 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.[60]

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

1. Each and every networked device is inherently vulnerable, i.e. leaking information.

2. All digitalized information, with an assignable monetary value, describing data subjects will be stored for an indefinite time and will eventually be processed.

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

37 To answer our question in section C, regarding creating trust for digital platforms, we think that the following definition of privacy could regain and maintain the individual user´s trust in digital platforms:

- Privacy should be a right for each data subject to actively and continuously monitor and control where and how data pertaining to the individual is stored, eventually processed, and by whom. Once data is intentionally shared outside the private sphere, e.g. in a status update or even when sensitive health data such as the genome is published, it becomes part of the public domain.

38 The remainder of the paper focuses on elaborating this definition.

39 Today, data subjects are often totally exposed to platform providers, and there is often little or no privacy in regards to a handful of global companies. This is enforced through complex privacy policies where users are forced to give up their rights and data protection laws are circumvented. These companies have gone to great lengths to create as complete profiles as possible on their users, by creating syndicates for registering information not only within their service, but also when a subject uses other companies that implement the same

57 See https://www.truste.com/resources/privacy-research/us-consumer-confidence-index-2015/ for further details. Accessed 10.02.2016.

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

59 Ibid.

60 Tilson, D., Lyytinen, K., and Sorensen, C. (2010). "Digital Infrastructures: The Missing IS Research Agenda," Information Systems Research (21:4), pp. 748-759; Henfridsson, O., and Bygstad, B. (2013). The generative mechanisms of digital infrastructure evolution. MIS quarterly, 37(3), pp. 907-931.

technology.[61] So far, the gathered information mostly contains behaviour related data for direct marketing purposes, but its future development is not limited to this. To mention a few examples of future prescriptive services: Google recently invested in a health insurance company;[62] Automotive companies (e.g. Tesla and Volvo) are about to launch semi-autonomously driving cars that they want to monitor continuously; and Uber wants to predict users' every need in regards to transportation,. The introduction of new Internet of Things data sources (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 digital 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 the consent contract has been signed. The definition is motivated by the data subject's capacity to choose an alternative platform service approach, which we find is lacking in the current Regulation proposal. 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 also lead to an improved competitive digital landscape in Europe.

I. Competition in Data Intensive Business

40 In the previous sections we put forth the argument that the network externality effect contributes to create de-facto monopolies in the digital world through the creation of "processing silos". We find that the fundamental reason for this is the immobility of data among service providers. Data immobility provides incumbents with a barrier to entry against new competition. User data has become a sought after resource that when traded forward for profit (supported by privacy policies) can cause users harm in some cases. As Pew Research[63] showed, in a large majority of cases, exploitation of user data causes uncertainty and confidence in service providers is weakened. Cerf and Quaynor[64] argued 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 among platforms such as social networks highlight this problem. Today, user contributed data is often locked in behind a service gateway connected to a service user ID.[65] For example, an open flow of data would imply that a tweet would show up on the Facebook feed for friends, and a status update on Facebook targeted towards the individual's professional activities would be shown on the user's Linked-in profile. These examples are trivial, yet illustrate how the significance of one service can be reduced and opened up for different types of services on a common platform. Today, many service providers have opened up certain APIs into their services, but to achieve true data mobility we believe a clear legal requirement is required. A mandatory separation of user data storage activities and service provider (processor) into separate legal entities would create the possibility for actual user data control, see figure 1. That services of similar nature could conform to the same platform standard is not implausible from a technological perspective, but rather other interests (e.g. business and sovereign) have so far prevailed. As an example, current social network platforms all share a common data structure, based on messages, user IDs, and relationships. Standardizing such a social networking platform should be fairly straightforward compared to the standardization efforts surrounding mobile communication networks.

41 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 an unconnected entity, new service innovation can be established in data storage solutions (data store).

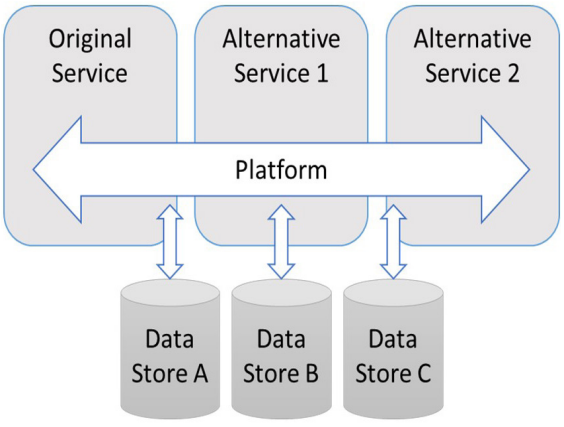

Figure 1- Separation of platform, service, and data store.

In extension, this should lead to a generalized solution where service providers would allow any

61 One such example is Google's Display Network that uses a technique referred to as Remarketing, which uses cookies placed in a user's web browser by other websites.

62 See http://venturebeat.com/2015/09/15/google-capital-makes-a-32-5m-bet-on-smart-health-insurance-company-oscar for further details.

63 Pew Research Center (November, 2014). "What Internet Users Know About Technology and the Web".

64 Cerf, V. G., & Quaynor, N. (2014). The Internet of Everyone. *Internet Computing, IEEE*, 18(3), pp. 96-97.

65 There are some decentralized online social networks e.g. Diaspora (https://diasporafoundation.org) or Friendica (http://friendi.ca) in addition to commercial alternatives that remain marginalised due to data immobility.

data store provider to provide the data store backend to a service. By using data store providers, consumers would have a natural point for storing and controlling all their consent contracts. This solution allows the user to determine the service and security level in a considerably finer grained fashion than today. If the data subject wishes to continue with a similar setup as today it would be possible, as a 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. Identity management can be handled in a similar fashion to email identities "user (at) domain". A similar authentication service is already in use for a world-wide roaming access service called eduroam,[66] which was developed for the international research and education community. The EU project FutureID[67] has developed a decentralized system for exchanging user ID credentials between different Internet services. Göndör et al.[68] also describe a system for migration of user profiles in the "SONIC Online Social Network Federation".[69]

42 These initiatives show that the technology is sufficiently mature to support a more user controlled privacy scheme that would support data mobility between platforms and services. What is currently missing are incentives for incumbent service providers to open up their platforms to decentralized services. Essentially, once a platform and service becomes a de-facto standard, a separation of the two are 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 the service.

II. Proposal

43 Brynjolfsson and McAfee[70] argue that we 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. In our paper we have argued for modifying the Data Protection rationale from a focus on the right to anonymity towards a Data Protection legislation based on individual control. If we want to achieve a safe digital societal inclusion, we also need a bridge between privacy policies and legislation. As we have illustrated in this paper, policies and legislation currently conflict with each other. Three proposals for consideration in a future EU Data Protection Regulation that would likely clarify the data subject's position in regards to platform privacy issues are outlined below. These proposals will also strengthen the competitive landscape, particularly with a focus on improving conditions for new diversified digital ventures and start-ups.

1. Modification One

44 One of the central modifications of the Data Protection Regulation ought to be aimed at lessening the ability of incumbent global actors to lock-in the user base to their platform. The rationale behind this is to enable true competition and a selection of differentiated services. The de-facto platform monopolies create a dangerous future where few companies can dictate or influence how the digital communities should behave as well as follow up how they actually behave. 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, any internal information sharing would not be allowed between said services. This, however, with the exception of some internal identity authentication 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.

45 Essentially this entails that Facebook for example, would not be allowed to share data subject generated data between WhatsApp and its other services without a public bidirectional API for both extracting and pushing user contributed data through the API. Correspondingly, Argenton and Prüfer[71] suggested a similar solution 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.

66 See https://www.eduroam.org/ for further details. Accessed 10.02.2016.

67 See http://www.futureid.eu for further details. Accessed 10.02.2016.

68 Göndör, S., Beierle, F., Kucukbayraktar, E., Hebbo, H., Sharhan, S., and Kupper, A. (2015). Towards Migration of User Profiles in the SONIC Online Social Network Federation, In the proceedings for The Tenth International Multi-Conference on Computing in the Global Information Technology, [accepted, forthcoming].

69 See http://sonic-project.net for further details.

70 Brynjolfsson, E., and McAfee, A. (2014). The second machine age: work, progress, and prosperity in a time of brilliant technologies. WW Norton & Company. pp. 123-124.

71 Argenton, C. and Prüfer, J. (2012). Search engine competition with network externalities, Jnl of Competition Law & Economics 8(1) pp. 73-105 doi: 10.1093/joclec/nhr018.

2. Modification Two

46 The second modification regards federated identity authentication and data stores, as defined in Section D.I. To limit the current unwanted tracking ability of syndicates, we propose that any authentication and data storing service is seceded from any processing entity. By separating the authentication ability and data store into a separate legal entity, it opens up innovation for new types of data storage solutions. By requiring a monetary based (not data based) transaction cost for the identification service, paid either by user 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 the cost is paid directly or indirectly in user data.

47 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.[72] This hinders provider control and sensitive data misuse by private companies. It is essential to ensure sender anonymity and an inability to link the message to a user 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, that when used can have a certain level of similarity to the true User ID, but offer 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 anonymize access to a public network.

3. Modification Three

48 The third modification concerns how security and data protection policies are reviewed. Achieving complete security is as probable as achieving full anonymity, as 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 proposed Regulation introduces a new role[73] 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) the person to be in a position to perform their duties and tasks independently; 3) liaising with regulators over personal data breaches; and 4) monitoring the performance of the data protection impact assessments of organisations. A mandatory position that can initiate internal security and policy auditing is a first and important step. The role will likely require a law degree for fulfilling the description of a data protection officer. This is similar to the role 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 within companies. In practice this would take the form of a compulsory 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.[74] If it is found later on that an auditor neglects their legally stated duties they would be held liable as well.

E. Conclusions

49 In this paper we have highlighted the problematic state of digital platforms implemented as "processing silos" with the support of privacy policies. We consider the present use of some privacy policies to be of a discriminative nature that foster the current privacy paradox environment. The inability to make use of a service is often hindered if the user does not accept the terms of the provider. These terms often require consent to transfer data between the provider's different services or require the sharing of data that can be considered excessive. The privacy paradox contributes to an uncertain digital service environment and a mistrust of anyone in a dominant

72 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, M., Wieschebrink, C. and Kugler, D. (2015). Public Key Infrastructure and Crypto Agility Concept for Intelligent Transportation Systems, In the proceedings for The Fourth International Conference on Advances in Vehicular Systems, Technologies and Applications [accepted, forthcoming].

73 Some criteria apply to the necessity of the role.

74 PWC (2013). Understanding a financial statement audit. Accessed 11.6.2015: http://download.pwc.com/ie/pubs/2014-pwc-ireland-understanding-financial-statement-audit.pdf.

position. Dominant position refers to an organisation that holds sensitive information of a personal nature on an individual and processes this information at it wishes. We provide three core proposals for a future Regulation that we believe would return trust in Internet services, including highly sensitive services built on Internet of Things technology. This will without a doubt require a closer cooperation between the legal community, companies, and technology standard-setting organisations. Neither party will be able to accomplish this challenging task alone.

50 We also find that start-ups (or any new digital service offering) and consumers alike are facing the problem that data is not transferred between services of companies. For example, why is a status update on a social media service not distributed to anyone outside the said service? A comparative service is email that can be transported across any Internet service provider platform. Hence, the limitation is not of a technical nature, but originates from what we consider to be a behaviour that strives to create a "processing silo" design. Whether these "processing silos" fulfil the definition of a monopoly in anti-competitive terms is beside the point when it comes to determining the platform privacy. Monopolies, regardless of nature, are considered by most scholars both competition and innovation averse in the long run. In the world of Internet of Things, they will also become omniscient. The ability to choose among platform providers should be considered a privacy right. A future platform regulation ought to target individual control-based Data Protection. Data subjects are very different in their ethos and this individuality needs to be addressed from a legal standpoint. We define a service objective for privacy that states that the data subject is always only a click away from both determining the status of his personal data and controlling the access to his data. The incumbent digital platforms are able to exploit their users' data as long as no real alternatives exist. We have made the argument that separating the platform from the service by having public APIs that allow for bidirectional communication and creating a federated identity authentication scheme would solve the current privacy issues described in the paper. An additional benefit of our proposal would be increased security, since data would only be unencrypted when processed.

51 In the future, data will be generated, collected, and processed in an ever increasing rate. Perhaps the greatest challenge will be to define a meta-structure for data to enable real-time communication between services. Data portability requires a common standard that is both flexible and robust, but as highlighted in the paper, data portability is not enough to mobilize data sharing between platforms or services.

52 As software increasingly encompasses all areas of life, there is a need for more focus on the security of data. We have proposed an audit procedure to supervise that the letter of the law is followed. As information systems mature there is a need for a more formal approach to security. An alternative to the audit process could be sizable penalties for breaches, but these penalties would become a risk to important services. Due to service scaling (millions of users), awarding each data subject a compensation representing an equal value to any breached personal data would in our view be too destructive to the individual companies. Hence we find the audit procedure to be a better alternative.

53 Inducing trust and social inclusion is of the utmost importance also in the digital world. In this area the European Union is the role model for regulators in the rest of the world. Open access to platform data is also highly important for companies in order to build competitive and differentiated alternatives to current services. This can be achieved through a separation of service and platform as suggested in this paper.

* Magnus Westerlund, MSc., is Programme Director in Information Technology at Arcada University of Applied Sciences and a Doctoral Student at Åbo Akademi University. Joachim Enkvist, LL.D., Ass. Prof. at Åbo Akademi University & Researcher at Luleå University of Technology.