Game-theoretical Model on the GDPR

Market for Lemons?

by **Tim Zander, Anne Steinbrück and Pascal Birnstill***

Abstract: In order to evaluate the regulatory effects of the GDPR on the institution of privacy as a public good, a data protection law and economical perspective should be applied. Conveying an economic point of view on the GDPR, we include a game-theoretical model on the rights and duties arising out of the GDPR in order to clarify the possible game-theoretical strategies and discuss the compensatory mechanisms for the problem of asymmetric information between the data controller and the data subject. Furthermore, we point out the concepts of control and the legal construction of "data ownership" as an unsatisfying concept. The fact that services within the scope of the GDPR can rewrite their privacy policies and afterwards request the users' consent or otherwise lock them out of the service causes undue pressure on the data subject. The recent decision of the Federal Cartel Office of Germany disputed this behaviour and imposed far-reaching restrictions on Facebook. Thus, elements of the GDPR have begun to fall within the remit of competition law and the question of effective regulatory compensation regarding the economic effects in privacy should be addressed. In general, the measurement of privacy risks seems to be the first reasonable step towards empowering actors to make effective decisions.

Keywords: EU-Privacy; game-theory; GDPR; justification of data processing; information asymmetry; adverse selection; network effect; lock-in effect

Recommended citation: Tim Zander, Anne Steinbrück and Pascal Birnstill, Game-theoretical Model on the GDPR - Market for Lemons?, 10 (2019) JIPITEC 200 para 1.

A. Introduction

1 The EU General Data Protection Regulation (GDPR) reflects a harmonised legal approach towards data protection law and the protection of personal data and privacy based on Art. 7, 8 EU-Charter in the European Union. The effectiveness of this Regulation remains to be subject to scrutiny. In general, the concept of privacy is linked to the idea of the *control* of private information[1] as the wording of recital 7 S. 2 GDPR states, "control of their own personal data". The question is, whether individuals have full control over their privacy or – if they wish to do so – can economically exploit their own personal data with the effect of a general disclosure of the common good *privacy*?[2] By taking a similar line of argument as *Anderson*,[3] who argues against the control concept on privacy, we reach the conclusion that markets of data processing might suffer from adverse

* Dr. Tim Zander, is research assistant at the Chair of Interactive Real-Time Systems at the Karlsruhe Institute of Technology; Anne Steinbrück, Ass. iur., is research assistant at the center for advanced legal studies at the Karlsruhe Institute of Technology and Dr. Pascal Birnstill is research assistant at the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB.

1 Laura Brandimarte, Alessandro Acquisti and George Loewenstein, 'Misplaced Confidences: Privacy and the Control Paradox' (2013) 4 Social Psychological and Personality Science 340.

2 Yoan Hermstrüwer, *Informationelle Selbstgefährdung* (Mohr Siebeck 2016) 134–38; Joshua AT Fairfield and Christoph Engel, 'Privacy as a Public Good' (2015) 65 Duke Law Journal 385.

3 Ross Anderson, 'Why Information Security Is Hard-an Economic Perspective', *Computer security applications conference, 2001. Acsac 2001. Proceedings 17th annual* (IEEE 2001).

selection due to network effects. Considering the risk-based approach in Art. 25, 32 GDPR, the question of quantified and qualitative measurement of data processing risks arises and requires the application of an interdisciplinary approach towards the phases of data processing. Thus, the game-theoretical model on the GDPR should be differentiated in four phases based on the life-cycle of data processing. With this analysis we provide a method for understanding the different levels of information players acquire during the life-cycle and the foundations of the decision-making process by the participating players.

B. Game-theoretical model on the GDPR

2 The general idea of the game-theoretic model is that the rules of the game are already implicitly defined in the GDPR. *Hermstrüwer* applied game-theoretic modelling in order to analyse the effectiveness of the GDPR in his dissertation.[4] However, the approach taken in the following article will point out the regulatory effects from a different angle. The model will be defined as an extensive-form game. The extensive-form means that the players carry out their actions in the game in a specific sequence. We can draw a finite extensive-form game as a tree (see for example Figure 1), where at each node a certain player has to take action and at the end of the sequence each player will receive a certain pay-out depending on the leaves as ends of the game-theoretical sequences. An important concept in game-theoretical modelling is the notion of information sets each player has. An information set is a set of nodes, which the player cannot distinguish, i.e. they do not know which actions have been taken by the other players. We can also take the beliefs of the players into account and extend the model to a dynamic Bayesian game. The players then will have beliefs about the likelihood of damages in the actual state of the game with each information set.

3 Games have certain types of feasible solutions, the so-called Nash-Equilibria. A Nash-Equilibrium can be seen as a stability point of the potential strategies of the players in the game, where no player has the incentive to deviate from his strategy. In the extensive-form games, where sequential actions are taken, the fact that players can change their strategy within the game has to be taken into account. The notion of Nash-Equilibrium is refined for this to subgame-perfect equilibria, or in the Bayesian-case perfect Bayesian equilibria, which are also Nash-Equilibria for every subgame.[5]

4 We will start defining the extensive-form game with the players. Players are of two general classes: the data subjects "D" and the controller and processor of a service "C". It would also be reasonable to include the supervisory authorities as players, but we omit this for the sake of simplicity. This is in line with the view of new institutional economics,[6] where the GDPR sets the rules of the game and the supervisory authorities would ensure their application rather than participating in the game, Art. 57 GDPR. Moreover, there are several supervisory authorities which may act differently as the GDPR leaves room for certain specification by the member states. The game is then divided into several phases. First, the preparation of the processing of personal data by C (B.I.), then the decision on consent and usage (B.II.), afterwards data processing under new circumstances (B.III.) will be analysed, and finally the rights of D (B.IV.) will be modelled.

I. Phase 1: Preparing the processing of personal data

5 To explain the basic action spaces in the game, we assume at this stage that there is only one controller and processor – C – and that they offer exactly one service. Furthermore, we assume that there is only a single data subject – D. The game starts with C setting the purpose for data processing with a service and the level of data protection to be implemented according to the state of the art, Art. 5, sec. 1 b), 25 GDPR. As the options are endless, we assume that for simplicity they have three options to set up the purpose and the level of protection, Art. 5 sec. 1 d), e), 25 GDPR.

6 Thus, C has to choose one of the following options:

1. A very restricted purpose beyond what is needed to satisfy the GDPR;
2. a purpose such that it just satisfies the GDPR; or
3. a very broad purpose such that it breaches the rules of the GDPR.

7 Then C has to decide the degree to which he will implement data protection according to the state of the art:

1. A high level of protection beyond what is needed to satisfy the GDPR;
2. a medium level of protection such that it just

4 Yoan Hermstrüwer, *Informationelle Selbstgefährdung* (Mohr Siebeck 2016).

5 Roger B Myerson, *Game Theory* (Harvard University Press 2013).

6 Douglass C North, 'Institutions, Transaction Costs and Economic Growth' (1987) 25 Economic inquiry 419.

satisfies the GDPR; or

3. a low level of protection such that it breaches the rules of the GDPR.

8 In general, it might be questioned whether C will optimise towards the best protection and a very restricted purpose due to the advantage of possibly discovering opportunities for financial profits with further data processing. At the same time, C will have the interest to reduce the risk of sanctions and a negative reputation. However, in case of a high-risk data processing, Art. 32 GDPR, a data protection impact assessment has to be implemented and executed. This includes the risk-based approach stating that C has to evaluate the risk of data processing regarding the rights and freedoms for natural persons in order to meet the necessary technological and organisational requirements, Art. 25 GDPR.

9 Due to the principle *"prohibition subject to approval"* in the GDPR, the processing of personal data requires the justification by C. Legitimised processing and the justification by C can be in particular based on:

1. Requesting the consent of the data subject, Art. 6 sec. 1 a) GDPR;

2. data processing is necessary for performance of a contract (e.g. terms of use), Art. 6 sec. b) GDPR; or

3. data processing is necessary for the purposes of a legitimate interest, Art. 6 sec. f) GDPR.

10 These grounds of legitimisation shall be a matter of documentation, Art. 5 sec 2 GDPR, and cannot be applied together.[7] Thus, the decision regarding legitimate grounds requires a diligent calibration of the risk involved with the processing as a compliance step.[8] From this point of view one might argue that the risk-based approach thus weakens the principle *"prohibition subject to approval"*,[9] as the review of the calibration might more easily lead to a justification based on the legitimate interest, Art. 6 sec. 1 f) GDPR, rather than applying legal grounds or requesting consent.

11 Consequently, C has to set up a privacy policy, Art. 12, 13 GDPR. Again, the model should be simplified by assuming that the players choose *write one and tell the truth*, *write one and not tell the truth,* or *do not write one at all.* If they choose to write the privacy policy, they again have a simplified choice to inform D about the purpose and the rights in a concise, easily accessible and understandable manner, recital 58, 59 GDPR:

1. in a clear and plain language such that it is very easy to understand;

2. in such a fashion that it just satisfies the GDPR; or

3. in such a way that it is not in compliance with the GDPR.

12 Here again C is likely to optimise the privacy policy in a manner to avoid possible sanctions and deterrence of D, instead of simply providing a privacy policy with a clear and plain language.[10]

II. Phase 2: Decision on consent or usage

13 The next decision by D is *to read* or *not to read*, and whether to *consult other sources* and then *confirm* or *decline* the privacy policy of the service. It is argued that serious costs might be associated with reading privacy policies, so it might be a reasonable decision by D in the game to not read the policy at all and either give the consent or not.[11] If D declines to consent to the privacy policy of the service, at a later sequence of the game D might provide the consent. In the decision process D might reflect the consent process and might also try to anticipate the value of the service as well as the associated risks, recital 39 GDPR. In general, the process of considering the consent by D is characterised by the informational asymmetry towards C.[12] Consequently it is impossible for D to foresee the risks regarding his privacy in the data life-cycle, as the privacy impact assessment is likely to be treated as a company secret and not as a matter of publication. Therefore, the likelihood of incompliance with the GDPR rules seems to be an everyday risk that D has to accept. Thus, the

7 Winfried Veil, 'Einwilligung oder Berechtigtes Interesse?: Datenverarbeitung Zwischen Skylla Und Charybdis' (2018) 71 Neue Juristische Wochenschrift 3337.

8 Claudia Quelle, 'Enhancing Compliance Under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502.

9 Winfried Veil, 'DS-GVO: Risikobasierter Ansatz Statt Rigides Verbotsprinzip-Eine Erste Bestandsaufnahme' (2015) 5 Zeitschrift für Datenschutz 347.

10 In the model depicted in Figure 1, we further simplify this by assuming that C tells the truth or does not write a privacy policy at all.

11 Omri Ben-Shahar, 'The Myth of the 'Opportunity to Read' in Contract Law' (2009) 5 European Review of Contract Law 1; Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 Journal of Law and Policy for the Information Society 543.

12 Yoan Hermstrüwer, 'Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data' (2017) 8 JIPITEC 9.

consent might actually qualify as a *reluctant consent*.[13] Assuming that the player D decides to consent and use the service, this has value for C as value might be generated through processing the personal data or the service might be acquired by another player.

14 On this basis the first game tree (Figure 1) includes the decision on the consent based on the information D received regarding the privacy policy or a prior data breach. The action of consent in the game-theoretical model consequently is the result of the reputation, the publicly available information and actions of C; namely, the information and the purpose for the processing. In general, due to the informational asymmetry D is likely to be limited in the evaluation of the potential risks.

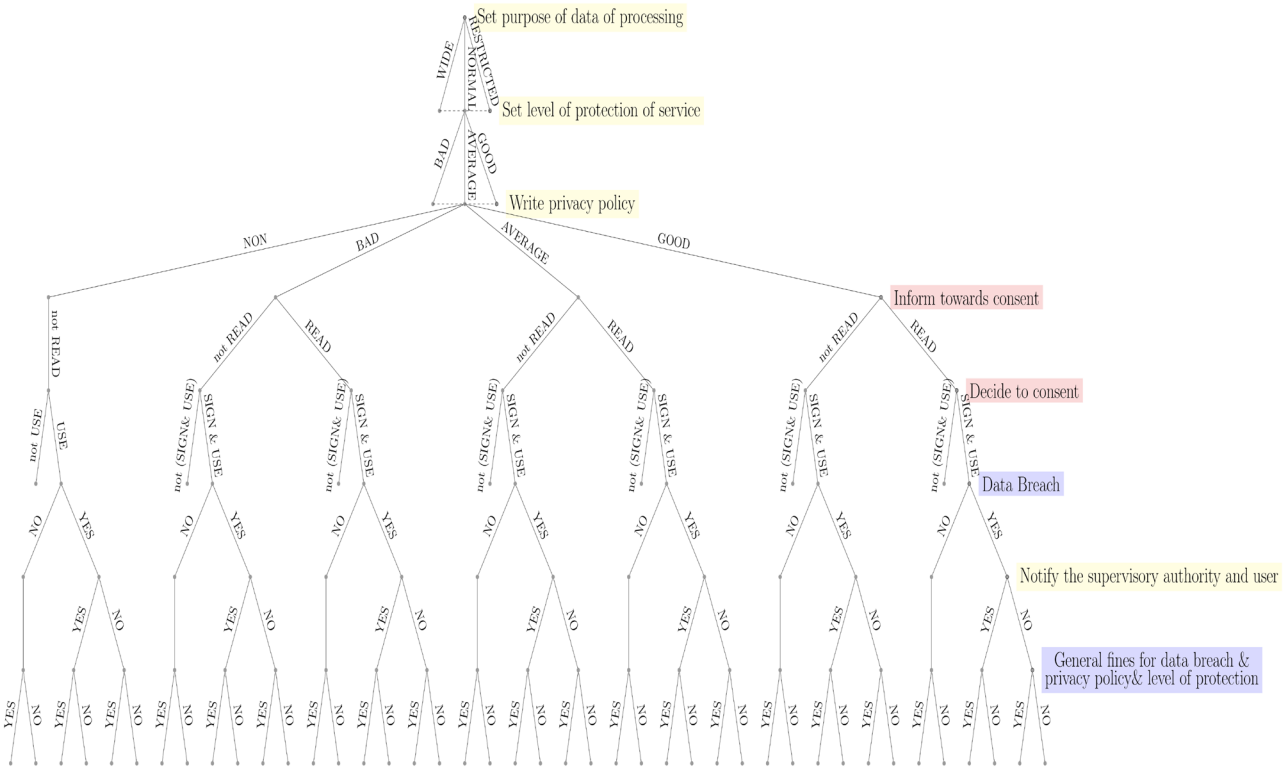

Figure 1: This depicts a further simplified game tree of the introduced model. Yellow belongs to C, red to D and blue is a move by nature.

15 In order to clarify that information regarding a data breach of C might not influence the decision-making process of D, it should be assumed from now on that multiple Ds are participating in the game.

1. Notification of a personal data breach influencing the decision

16 In case of a data breach, which can be modelled as a random event in the game (move by nature, see Figure 1), C has to notify the data breach to the supervisory authority without undue delay, Art. 33 sec. 1 GDPR. Also, C shall comprehensively document all facts of the personal data breach and in case the data breach causes a high risk to the rights and freedoms of natural persons, C shall communicate the data breach to D, Art. 34 sec. 1 GDPR, otherwise they may face fines. This mechanism also works to some extent against the information asymmetry between C and D. From our game-theoretic model (see Figure 1) we can draw the conclusion that the compliance with this procedure can depend on the likelihood of the fines. In general, although a data breach and the notification of the supervisory authority might be in place, the question remains whether D might choose another service as other Ds (data subject players) keep using the previous service by C. Moreover, D might be affected by network and lock-in effects, thus a privacy preserving decision becomes even more difficult.

13 Philip Radlanski, *Das Konzept der Einwilligung in der Datenschutzrechtlichen Realität* (Mohr Siebeck, 2016) 162.

2. Network effects within the decision-making process

17 We first note that the decision of whether to accept a privacy policy and use a service or not could be interconnected with the decision of other Ds. Take the example of a messenger. Then the decision to use one messenger over another one depends on the other Ds one wants to communicate with. Based on the correlation between the number of other Ds and the influence on the decision-making process, this can explain the high value of services by some Cs. This effect is the so-called network effect. Under network effects the privacy decision of D for a service with a poor reputation on privacy settings can be based on a rational choice including the evaluation of the advantages and disadvantages ending with the consent and the usage of a service. This might even be the case if D has a high interest in protecting privacy, as the network effect can potentially outweigh any perceived negative consequence.[14] This can be illustrated by the example of two messenger services with different levels of privacy and popularity; for example, one service may have poor privacy technology but it is more popular amongst your peer group and another service may have a high level of privacy technology but none of your peers use it. Then the evaluation of this boils down to whether to use the messenger with poor privacy or not. The non-usage might have significant social consequences, and on the other hand usage has a high impact on the privacy of many Ds. Considering these findings with regards to the privacy paradox phenomenon, it might be argued that the Ds are very limited in their decision-making process due to network effects, i.e., although they might have a high interest in their privacy, they may choose higher levels of social interaction over their privacy concerns.

18 The difference between GDPR rules and the criterion of effective actions can also be illustrated by applying *Shakespeare's* Romeo and Juliet to a modern setting. They love each other but their families are in serious dispute. Thus, each of them would face serious social consequences if her or his family would find out about it. As they recently began their relationship and they are not sure for now whether it would be worth it to publicly announce their love, they decide to keep it secret. Of course, they are equipped with the wonders of modern communication such as smartphones and social media, and they start to consider how their personal data could potentially reveal their relationship. They would worry about being tracked down by their relatives *via ad* targeting for surveillance.[15] So now it gets tricky, as many of the services are already aware about the fact that Romeo and Juliet know each other and meet on a regular basis. Even more, they suspect – with high probability – that they are lovers.[16] So special ads are placed on their social media page, such as those from local flower-shops. Sooner or later it happens that one of the members of the house of Capulet will see an advertisement on Juliet's phone and dramatic events would ensue. We ask whether this drama could have been prevented by reading the privacy policies. We suspect that this is not the case and hence view this as another example of asymmetric information towards D.

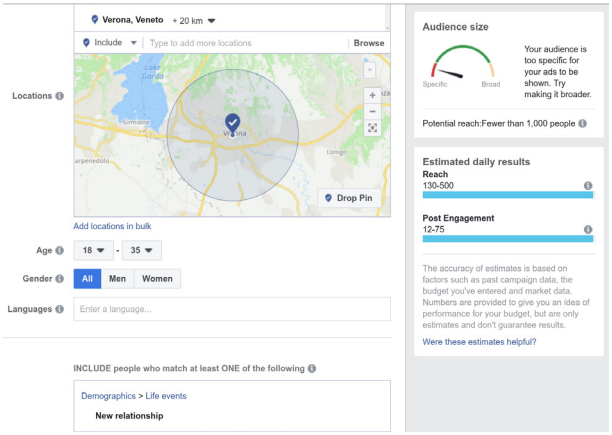

Figure 2: Facebook's advertisers' tool for defining target groups: Romeo and Juliet example

19 In the next subsection, we will focus on asymmetric information, which might lead to a market where only services with poor privacy properties prevail. This type of market behaviour is known as adverse selection.

III. Phase 3: Pursuing the data-processing under new circumstances

20 In this subsection the game-theoretic model will be simplified in order to concentrate on one problematic aspect leading to an adverse selection in the market. The simplifications we are making will be aggregated in Figure 2. Consequently, a specific

14 Zsolt Katona, Peter Pal Zubcsek and Miklos Sarvary, 'Network Effects and Personal Influences: The Diffusion of an Online Social Network' (2011) 48 Journal of Marketing Research 425.

15 Paul Vines, Franziska Roesner and Tadayoshi Kohno, 'Exploring Adint: Using Ad Targeting for Surveillance on a Budget-or-How Alice Can Buy Ads to Track Bob', *Proceedings of the 2017 on workshop on privacy in the electronic society* (ACM 2017).

16 Carlos Diuk, 'The Formation of Love' <https://www.facebook.com/notes/facebook-data-science/the-formation-of-love/10152064609253859/> accessed 2 September 2019.

type of service processing personal data, such as a messenger, a social network or a fitness tracker, should be applied. Assuming that at the beginning of the game each service has a restricted purpose for processing personal data, a good level of data protection, and a well-written privacy policy. Also, it should be assumed that every individual has read the privacy policy. Now the usual decision has to be made by D whether or not to consent and use a particular service. As the service could reset the purpose of data processing in the new privacy policy to the more general level in a compatible manner and could also change the level of data protection applied for the processing, the protection of the rights and freedoms of the natural person might be at risk. Considering network effects or lock-in effects, D is likely to consent to the amendments made by C or continue using the service based on the legitimate interest. In these new circumstances D cannot foresee the alterations by C and the situation of information asymmetry is becoming reinforced. In particular the acquisition of an enterprise such as WhatsApp by Facebook can lead to an increase of information asymmetry and thus to adverse selection. If the costs to terminate or switch the service are too high for D (lock-in effect), then D is likely to remain with the service, even under deteriorated privacy circumstances. The case of high costs for switching services is also due to network effects. With applying the opportunity to sign and continue using the service, D cannot foresee these alterations by C and the situation of information asymmetry becomes reinforced. Other factors, such as economic necessities of the service to use the data for advertisement in order to become profitable also cannot be foreseen by the data subject D and often not even by the service provider C. Consequently, the strategy of C will likely focus on getting as many Ds as possible by potentially investing in advertisement, maybe even pointing out a high degree of privacy.[17]

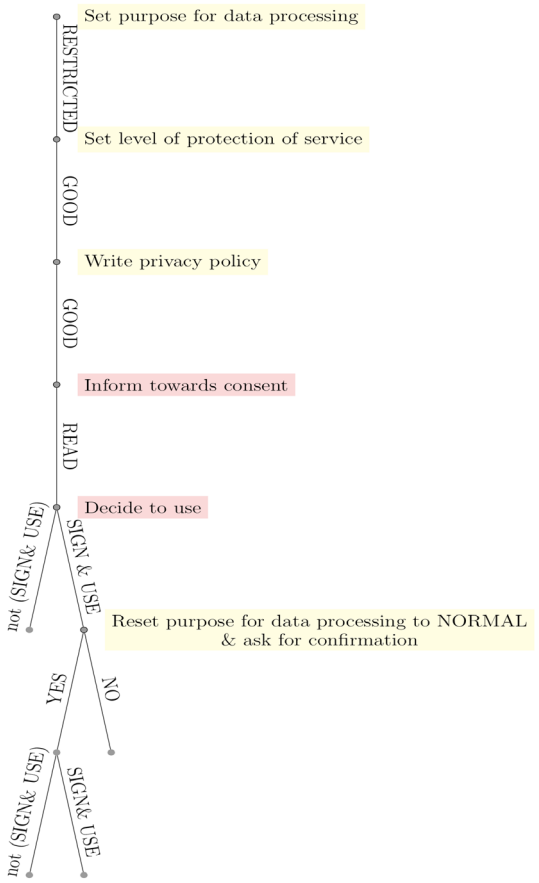

Figure 3: Actions sequence leading to adverse selection (simplified)

21 The phenomenon regarding the high cost of switching to another service or product is known as the lock-in effect. For example, software and software-as-a-service businesses,[18] where the value of the companies is closely tied to the lock-in effect. In fact, the monetary value of a company can be estimated by summing up all of its users' switching costs.[19] In addition, software can be tightly interconnected with the hardware, as it is the case with many technologies such as fitness trackers, smart TVs, speakers for virtual assistants and smartphones. The costs of the hardware are added to the switching costs, if the hardware and the data processing are tied to the software.[20] The software and the software-as-a-service run on these smart devices and their corresponding servers are responsible for processing the personal data of the subjects. This means that if D is locked-in to a software

17 Lifang Zhang, 'Lock-in Strategy in Network Industries: A Network Effect Perspective', *2009 6th international conference on service systems and service management* (2009).

18 Sonja Lehmann and Peter Buxmann, 'Pricing Strategies of Software Vendors' (2009) 1 Business & Information Systems Engineering 452.

19 Carl Shapiro and others, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business Press 1998) 108, 116.

20 Joseph Farrell and Paul Klemperer, 'Chapter 31 Coordination and Lock-in: Competition with Switching Costs and Network Effects' in M Armstrong and R Porter (eds), vol 3 (Elsevier 2007).

and software-as-a-service, which processes personal data, then it is also locked-in to the processing of their personal data by the proprietor of the software. In order to illustrate adverse selection in these circumstances, the Akerlof's famous example of the used car market[21] can be adapted.[22] It can be shown that in some markets of services processing personal data, D is likely to be nudged to accept the privacy policy with the broader purpose of processing and thus weaken the level of privacy protection. The following questions then arise: to what extent can legal mechanisms compensate these market effects and whether the GDPR might even encourage such market effects with the explicit regulation on permitting the amendment of purposes in Art. 6 sec. 4 GDPR.

22 Moreover, network and lock-in effects have a strong interconnection.[23] Recently, this led to an intervention by the German Federal Cartel Office on Facebook. The Federal Cartel Office argued that only based on a voluntary consent by the data subject D, the data sets of Facebook, WhatsApp and Instagram might be connected, otherwise it must be internally unbundled.[24] Due to Facebook's market-dominating role, the freedom of consent was questioned by the agency and consequently, whether the consent was a result of free decision-making or if it was an illegitimate *reluctant consent*. Furthermore, it was stated that due to combining of the data, the C strengthens the market dominating role and individual data gain further significance, which the user cannot foresee.[25] The Federal Cartel Office essentially recognised the asymmetric information between the players and market dominating position. This decision might set a strong precedent against market leaders and, in interaction with other authorities, lead to recognisable change regarding the interconnection between data protection law and competition law. Having demonstrated the economic effects of the GDPR and the fact that data protection law has also become a matter of interest to the authorities on competition law, attention should be drawn to Art. 20 GDPR.

IV. Phase 4: Rights of the data subject

23 In Art. 15-21 GDPR the rights of Ds are regulated. The primary right is the right of access stated in Art. 15 GDPR, which allows D to receive the information regarding the earlier data processing conducted by C in order to take the next steps. After obtaining the relevant information on the data processing, D might decide to make use of the right to rectify the stored information, Art. 16 GDPR, or the right to erasure, Art. 17 GDPR. The right to erasure also known as the "right to be forgotten" is based on the decision by the European Court of Justice *Google Spain SL v Gonzales.*[26] Even though the incorporation of this judgment in the GDPR might seem appealing, it is argued that in times of ubiquitous computing the right to erasure is burdensome to realise, thus a reversal of the burden of proof in a manner that C has to prove the erasure "with best effort" of the personal data is proposed.[27] Further, the perceived control could tempt the data subjects to be less sceptical and make the use of their personal data more effective.[28] Another option D has, is to request the restriction of processing based on Art. 18 GDPR in cases of unlawful or inaccurate processing. Also, D has the right to object to the data processing at any time based on Art. 21 GDPR. These actions might be chosen by D:

1. Right of access, Art. 15 GDPR;
2. Right to rectification, Art. 16 GDPR;
3. Right to erasure, Art. 17 GDPR;
4. Right to restriction of processing, Art. 18 GDPR;
5. Right to data portability, Art. 20 GDPR;

21 George Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism', *Uncertainty in economics* (Elsevier 1978).

22 Details from a mathematical perspective: If the market will consist of service providers "*p*", the percentage of them will change the purpose of processing personal data of a smart device to *NORMAL* at some point in the future. The long-term costs for enterprises are 160 for a product with a *RESTRICTED* purpose and 80 for products with a *NORMAL* purpose, e.g. those who use the data for advertisement. Assuming that for the buyers the *RESTRICTED* product is worth 200 and the *NORMAL* 100, as the buyers cannot differentiate between services that will change their purpose for the worse and the ones that will not, the price a buyer is willing to pay is the expected value of the product. Now it is likely that the price data subjects are willing to pay is less than 160.

23 Carl Shapiro and others, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business Press 1998) 108, 116, Chapter 7; Lawrence G Sanders, *Developing New Products and Services* (Saylor Academy, Open Textbook Library 2012) Section 10.1

24 *Bundeskartellamt*, the German Competition agency, 'Case report, 15.02.2019, Reference Number B6-22/16' <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4> accessed 2 September 2019.

25 ibid 12.

26 Judgment in *Google Spain SL v Gonzales,* C-131/12 [2014] ECJ, 13 May 2014.

27 Indra Spiecker gen. Döhmann, 'Steuerung Im Datenschutzrecht – Ein Recht auf Vergessen wider Vollzugsdefizite und Typisierung' (2014) Kritische Vierteljahresschrift 28.

28 Catherine E. Tucker, 'Social Networks, Personalized Advertising, and Privacy Controls' (2014) 51 Journal of Marketing Research 546.

6. Right to object, Art. 21 GDPR.

24 Now if D chooses to take one or more of the stated actions, then C has to respond to them according to the terms of the GDPR. The focus now will be on effects of these rights and in particular of the right to data portability in the game-theoretical model.

1. Data Portability and lock-in effects, Art. 20 GDPR

25 The purpose of the right of data portability is on the one hand to limit lock-in effects in the market by providing D a right to potentially switch from one service provider to another and on the other hand to provide a higher degree of privacy and consumer protection, Art. 7, 8 EU-Charter.[29] Whenever switching to another service is associated with significant costs for D, then a lock-in effect is in place. In order to circumvent such a significant attachment of D to a service, the choice to switch the service should be made easier by providing a particular data portability right, Art. 20 GDPR. However, the question arises to what extent this right empowers D to "take" the personal data to another service provider. As the wording of Art. 20 sec. 1 GDPR permits the transmission of "provided" data, this might exclude personal data that is generated by C such as profiles.[30] Considering the impact profiles can have during a data life-cycle, the current wording of Art. 20 GDPR seems too narrow to fully compensate lock-in effects and empower the user to switch the services.

2. Ownership on data?

26 Applying an economic point of view,[31] stating that in a data market the case of the *"user owning data"* will lead to the best equilibrium in terms of general public welfare and the public good privacy. Hence, a service provider C, that would support Ds to execute their data subject rights and additionally support Ds to offer their personal data on a market, might generate a surplus for the public good privacy. However, the concept of *ownership on personal data* is incompatible with the current data protection concept in the GDPR, based on the European concept to protect personal data, Art. 7, 8 EU-Charter. The concept of ownership would imply an absolute right with *erga omnes* effect, which could hardly be applied to personal information as they are intangible and relative. Also, the ownership on personal data would have to be a matter of bargain and a matter of relinquishment of ownership,[32] where it needs to be questioned how the legal concept could look like. Generally, in European and also in German law, the concept of privacy is directly linked with human dignity and cannot be a matter of absolute rights, which might be sold or given up as personal data are matter of a communication process and therefore relative. Even though an economic concept of ownership on data seems appealing at the first glance, after scrutiny it fogs up the legal structure and principles of the GDPR and data protection law in general.[33] Instead of the ownership concept it is widely perceived that data protection rights are a matter of access and could be transferred into a legal structure of granting and limiting access rights.[34]

C. Mechanism of Solution: Law or Market?

27 The question arises regarding how a solution might look like. It can be noted that the concepts of privacy by design and security by design based on the legal principle of state of the art, Art. 25 Sec. 1 GDPR, also aim to control technological development. However, *Schallbruch*[35] argues that technological phenomena such as Alexa or fitness trackers as a part of the "digital household" are predominantly influenced by free market competition rather than the legal principles. Consequently, a lack of transparency and understanding on how the new technologies actually work is a result of market power. Hence, we have to acknowledge that the privacy problems associated with the use of certain services is not only a concern to privacy laws but also a subject applicable to competition laws, as argued above. These regulatory mechanisms will of course not circumvent the problem of asymmetric information in terms of the scope and security of processing personal data. Here a closer look is required, whether

29 Winfried Veil, in: Sybille Gierschmann and others, '*Kommentar Datenschutz-Grundverordnung*' (Bundesanzeiger 2017) Art. 20 GDPR, para 3, 6.

30 Ruth Janal, 'Data Portability-A Tale of Two Concepts' (2017) 8 JIPITEC 59.

31 Charles Jones, Christopher Tonetti and others, 'Nonrivalry and the Economics of Data' (2018) <http://christophertonetti.com/files/papers/JonesTonetti_DataNonrivalry.pdf> accessed 2 September 2019.

32 Václav Janeček, 'Ownership of Personal Data in the Internet of Things' (2018) 34/5 Computer Law & Security Review 1039.

33 Jürgen Kühling and Florian Sackmann, 'Rechte an Daten', 25 <https://www.vzbv.de/sites/default/files/downloads/2018/11/26/18-11-01_gutachten_kuehling-sackmann-rechte-an-daten.pdf> accessed 2 September 2019.

34 ibid 31; Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) 4 J. Intell. Prop. Info. Tech. & Elec. Com. L. 257.

35 Martin Schallbruch, *Schwacher Staat Im Netz* (First Edition, Springer 2018) 181.

the sanctions are sufficient such that non-compliant conduct does not pay out. Another option to consider would be to legally force communication services to open up interoperability, such as telephone companies who cannot forbid users to call or be called by anyone using another provider. The same should be technically possible for most proprietary communication networks.

D. Conclusion

28 We have provided a game-theoretic model using the rules set by the GDPR. We discussed how information asymmetry affects the decision-making process on free consent. Then we concluded that together with network effects or lock-in effects this information asymmetry leads to adverse selection. Based on these findings it can be concluded that data protection law is also exposed to market effects, as it is the matter of Art. 20 GDPR. This leads to the conclusion that due to the market mechanism the public good privacy is at a higher risk than the regulations of the GDPR might be capable to compensate for. Furthermore, it could be demonstrated that legal concepts of control or ownership on data might not provide a higher degree of data protection, but attention needs to be drawn to the access of information. The multifactorial effects the consent and legitimisation might have on a service during a data life-cycle illustrates the need for interdisciplinary work on how to measure the privacy risk for individuals as the public good of privacy in the democratic process might be at stake. In particular, one could develop a method, which takes these economic aspects into account and evaluates the risk to the data subjects. Such a method might lead to an evaluation of risks for the individual, the democratic society, as well as the market of data[36] and provides the grounds for transparency to all players. This might be a differentiated scheme regarding access rights based on a concept of *"collaborative common"* as *Rifkin*[37] states, or *datapool* as peer based non-profit service providers[38] might offer. Such a concept might provide a solution on an individual behavioural basis and influence the market mechanism.

36 Stefan Drackert, *Die Risiken der Verarbeitung Personenbezogener Daten* (Duncker & Humblot 2014).

37 Jeremy Rifkin, *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism* (St Martin's Press 2014).

38 Yochai Benkler, 'Coase's Penguin, or, Linux and "the Nature of the Firm"' (2002) 112 The Yale Law Journal 369; Yochai Benkler and Helen Nissenbaum, 'Commons-Based Peer Production and Virtue' (2006) 14 Journal of Political Philosophy 394.