Internalization of privacy externalities through negotiation

Social costs of third-party web-analytic tools and the limits of the legal data protection framework

NILS WEHKAMP

Digital Society Institute of European School of Management and Technology Berlin, Germany nils.wehkamp@esmt.org

Tools for web-analytics such as Google Analytics are implemented across the majority websites. For most cases, the usage is free of charge for the website-owners. However, to use those tools to their full potential, it is necessary to share the collected personal data of the users with the tool-provider. This paper examines if this constellation of data collection and sharing can be interpreted as an externality of consumption in the sense of welfare economic theory. As it is shown that this is the case, the further analysis examines if the current technical and legal framework allows for an internalization of this externality through means of negotiation. It is illustrated that an internalization through negotiation is highly unlikely to succeed, because of the existence of information asymmetries, transaction cost and improper means for the enforcement of rights of disposal. It is further argued that even if some of those issues are addressed by data protection laws, the legal framework does not ensure a market situation necessary for a successful internalization. As a result, the externalities caused by the data collection through third party-web-analysis tools continue to exist. This leads to an inefficient high usage of third-party tools for web-analytics by website-owners.

CCS CONCEPTS •**Security and privacy~Human and societal aspects of security and privacy~Economics of security and privacy**•Information systems~World Wide Web~Online advertising•Applied computing~Law, social and behavioral sciences~Law

Additional Keywords and Phrases: Consent, GDPR, Google Analytics, coase-theorem, Data economy, Web-Analytics

ACM Reference Format:

First Author's Name, Initials, and Last Name, Second Author's Name, Initials, and Last Name, and Third Author's Name, Initials, and Last Name. 2018. The Title of the Paper: ACM Conference Proceedings Manuscript Submission Template: This is the subtitle of the paper, this document both explains and embodies the submission format for authors using Word. In Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY. ACM, New York, NY, USA, 10 pages. NOTE: This block will be automatically generated when manuscripts are processed after acceptance.

1 Introduction

The usage of third-party web-analytic tools like google analytics is one of the main reasons for the need of user consent when visiting a website. Those tools allow the owner of a website to gain information about the behavior of its users which can be used to further improve the structure, function, and workflow of the site according to its purpose. The use

of third-party web-analytic tools allows even more elaborate scenarios, like cross-site tracking, which enables a wide variety of marketing-analysis use cases, such as conversion tracking of personalized advertisement. The use of a third-party web-analytic tool appears to be attractive for the website-owner in a double sense. First, he profits from the larger knowledge production, which is possible through the extended data pool from the provider of the third-party tool. Second, he usually has lesser implementation cost, because the technical quality of the third-party tool is better than most of the website-owners could reach when using self-developed solutions [54; 52]. The usage of the third-party tool is usually free of charge for website-owners up to a certain point. The provider of the tool profits through the collected and shared data, by monetizing it for personalized advertisement [48].

Using this business-model, third-party web-analytic tools were able to establish themselves on a huge fraction of existing websites, especially commercial ones [8]. Even though legislative measures, e.g., the GDPR, require the consent of the user for its data to be shared and used for advertisement purposes, the use of those tools does not seem to decline. On the contrary, the website- owners seem to be willing to invest great efforts into designing the now infamous “Cookie-Walls” to get the required consent. While the benefits for the website-owners are obvious, it seems that the user is “paying” the cost for the website-owner by providing his personal data. This phenomenon, when something is consumed at the expense of someone else, is described as externalities, which lead to an inefficient market result. Furthermore, the welfare economic theory formulates requirements, under which the related parties resolve the externality by negotiation (coase-theorem).

The aim of this paper is to analyze the businessmodel of providing a free of charged third-party web-analytic tool for the website-owner, in exchange for sharing the user-data for its welfare economic implications. First this paper examines if externalities occur through the collecting and sharing of the user-data, while the provided benefit is consumed by the website-owner. Based on this analysis this paper furthermore examines if the current legislative data protection measures implemented within the European Union, are suited to internalize possible externalities through negotiation.

2 Solutions for dealing with externalities within theory

Externalities do not only raise moral concerns of fairness, but also cause the inefficient use of resources, which is an undesired result within the welfare-economic theory. Therefore, the existence of externalities causes the need for action, which means they must be internalized through appropriate measures. To ignore existing externalities would cause marketfailure, while the absence of regulative measures to prevent this means state-failure (while those terms must be interpreted as technical categories within welfare economic theory without moral implications) [55]. To internalize here means, that the consumer of goods is made to consider the overall costs within his consumer-function [65]. Possible solutions in the welfare-economic theory can roughly be categorized in public measures (marked-based or legislative-based), private measures and mixed forms [34].

Prime example for marketplace public measures is the Pigouvian-tax. This solution relies upon taxing the production or the consumption of the goods that produce the externality. The amount of tax to be imposed is equal to the amount of the social costs. This way, the producer of the externality must consider the social costs within his production- or consumption- function and the efficient market equilibrium is restored. The revenue of the tax can then be used to compensate the third party (or third parties) that bears the social costs [7].

Legislative measures include the ban and prosecution of the action that causes the externality. That does not mean that the production or consumption of the associated good must be prohibited at all, only the real actions within the production/consumption as a cause [38]. Looking at the example of the laundry, a solution would be to prohibit to dispose the sewage into the river.

Private measures include the establishment of social norms or creating a self-interest within the party causing the externality. An example for a social norm would be the trend to present yourself as a company as green and ecofriendly [21]. In this case, the laundry-owner would think about another way to dispose his sewage, because he would fear an image backslash if the pollution of the river would be discussed publicly. A self-interest could also simply exist because the laundry-owner lives down the river himself.

There are also mixed forms of public and private solutions. The most important form is the legal assignment of ownership rights (or comparable rights like rights of disposal), which enable the involved parties to negotiate contractual solutions [12].

A widely acclaimed theory for internalization through market mechanisms (in combination with rights of disposal) is the coase-theorem. Coase [1960] argues that even if externalities exist, an efficient allocation of resources and thus an efficient marked outcome is possible through negotiation of the involved parties. For example, the owner of the laundry could offer the fisher down the river compensation if he agrees to accept the pollution through the disposal of sewerage into the river. The compensation, that the fisher would be willing to accept, would be equivalent to his damage caused by the disposal. Within the coase-theorem it explicitly does not matter which party initially holds the rights of disposal. Even if the fisherman pays the laundry owner for not disposing his sewage into the river, the negotiation will result in an efficient market outcome. The requirement is the possibility for a successful negotiation, while aspects of fairness are not considered. Within the negotiation requirements for perfect markets apply, otherwise improper pricing would affect the efficient market outcome. Transferred to online information markets Noam [1994] summarized the requirements as:

- Sufficiently low transaction cost
- A legal environment that permits transactions to be carried out
- An industry structure which permits transactions to occur
- Symmetry of information among the transacting parties
- The ability to create property rights, or to exclude

Applied to the use of tools for web analysis, internalization through a Pigouvian-tax is not a candidate for a solution, because tax laws addressing this issue currently do not exist. Also, a private solution through social norms seems to be unlikely, not only because Google discarded it's Company "Don't be evil" [4], but because of its market power. This paper wants to focus on the internalization through negotiation. Even though the coase-theorem is widely criticized as being unrealistic, especially because of the assumption of no existing transaction cost and information asymmetries, the technological possibilities of the internet seem to provide such requirements more than any prior markets [46]. On the other hand, this paper does not want to promote a fully laissez-faire online-market, as could be deducted using the coase-theorem, but use the formulated requirements of the coase-theorem for successful negotiation to analyze, if the current data protection framework is suited to promote successful internalization.

3 Identification of externalities within the use of web-analytic tools

As the theoretical background is covered, this chapter is going to examine whether there is an externality within the use of web-analytic tools. This paper uses Google Analytics as a subject for the empiric observation, as Google Analytics is one of the most established tools on the market [68]. Within this chapter, the scope of functions of Google Analytics is examined, whether the use of it causes externalities.

3.1 Scope of Functions and Business Model of Google Analytics

Google Analytics is the web-analytic tool of the Company Google LLC. (represented by Google Ireland Limited within the European economic area) and part of its marketing platform suite [23]. Its main use for the users (mostly website-owners) is to gather and analyze the usage behavior on its website. This enables the owner of a website to perform analyses for various purposes, especially for reasons of optimization [25]. To gather behavior data, the owner of the website implements so called event-trackers. Those trackers are scripts which are implemented on the website, that are triggered once the specified user action is performed. An example of captured events can be clicking on a sub-link or scrolling behavior [29]. To enable the tracking of consecutive events performed by a website-user, cookie-technology is used by Google Analytics. By using this technology, Google Analytics assigns a pseudonym identification number, that can be assigned to the individual performed actions [25]. The website-owner is not able to reconstruct the individual user behavior on an individual user level (even not in aggregated form). The gathered information is presented to him in form of statistical aggregated form of reports [26].

Google Analytics can be used just to track user behavior isolated on one website. However, the much greater appeal of the tool is to integrate it in the bigger context of the Google Marketing platform. There are different ways and use-cases doing that, which all involve sharing at least part of the user-data that are collected on the website itself with Google. This sharing enables the connection of this data with the data pool Google has accumulated through its other services. This enables especially the tracking of users across websites, with significantly increases the information value of the produced reports. One example for this is information about the demographics of website visitors [28]. Another major use-case for cross-site tracking is the conversion tracking of online advertisement. If a website-owner also uses the services of Google to distribute advertisement, the connection of those two services within Google's marketing platform enables website-owners detailed insights about the behavior of user clicking on the ads. By knowing which ads were most effective, elaborate optimization methods for marketing campaigns are made possible [30].

To benefit from the foremost mentioned extended reports which rely on the extended data pool, the website-owners must willingly consent to the shared use of the collected data and allow Google to use the data for its own purposes [27]. Otherwise, the collected data is technically processed within the technical infrastructure of Googles services, but logically separated and not used by Google for its own purposes. If the website-owner agrees to share the data, possible necessary user consents must be obtained by the website-owner [31].

The use of Google Analytics is free of charge for the website-owner to some extent. According to the end-user-license-agreement, the free use applies until an amount of 10 million recorded tracking events [32]. Google does not publish official data on the share of paid and unpaid users, the free model seems to be suited for most websites [16]. Although Google does not publish official pricing numbers. Reports in dedicated marketing forums and blogs give a range from about 1135000 – 150000 $ annual charge [61].

For the further analysis, it is assumed, that the website-owner agrees to share the collected data with Google. Therefore, the application of Google analytics can be summarized from a market perspective as follows:

The website-owner uses Google Analytics on his website. He collects personal data from the website user and gains benefit from it. He shares data with Google, which in exchange can provide the tools.

3.2 Does the collection of the personal data of the user qualify as externality?

The use of third-party web-analytic tools may qualify as an externality within consumption. The good to be consumed is the web analytic-tool by the website-owner. At first sight, the use of Google Analytics by a website-owner clearly seems to qualify as an externality, because the website-owner gets a tool basically for free while the website user "pays" with his personal data. But to be interpreted as actual costs, the data collection must impact the website user in an actual negative way. To examine if the data collection actually implies a negative impact on the user, this section takes a look at two different ways of interpreting the act of collecting personal data. First, it is examined if personal data can be treated as a classical commodity or asset. The second subsection discusses if the impact of data collection on the privacy of the user can be interpreted as cost.

3.2.1 Data as commodity.

The simplest way to constitute an externality would be, to treat the collected data as an asset. If this asset first "belongs" to the data subject and then would be transferred to the website-owner, who then shares the asset with the provider, the transfer of the asset would clearly imply costs for the data subject. However, the economic characteristics of data do not automatically imply a loss on the side of the data subject, even if the collector of the data profits from the collected data itself and non-rival in its consumption as well as initially non-exclusive [48]. This means that data generally can be endlessly reproduced and the use by one party does not mean that the data is used up and cannot be used again. So especially the collection of personal data does not result in a situation, where it cannot be used or collected again, either by the data subject or another data collector. As a result, there is no commodity or asset, that is taken from the data subject.

In the literature, there are opinions that see data as an intangible asset. Those opinions and associated discussions about "data ownership" [39] within the legal literature, rather refer to a collected body of data, and not to the act of collection itself [41]. As a collected body of data can be used, as well as be traded, e.g. in the form of access rights, this

body contains an economic value for its owner. The value rather does not originate from the pure existence of personal information about a data subject, but in the embodiment of the data in digital form (as well as the context within a large collection of data subjects). This value is hard to realize for the single data subject itself. Therefore, the sole act of collecting data using a web-analytic tool cannot "take away" the data itself as a commodity.

As a result, costs and therefore an externality cannot be established by treating data itself as a commodity.

3.2.2 *Privacy as commodity.*

Even if the data itself does not inherit a value for the data subject, the collection of it impacts the dimension of information privacy. The concept of privacy is broadly discussed across fields (for an overview see e.g. see Smith et. al. [2011], Pavlou [2011], Acquisti, et. al [2016]) and can generally be described as the control of an individual about the intrusion in its personal space. Information privacy is therefore affected if personal information is collected and used. From an economic perspective, the impact on information privacy can be qualified as costs, because it causes either objective or subjective negative consequences of the collection and use of personal data.

Objective negative consequences are negative impacts through the actual use of personal data. The data collected through web-analytic tools are mainly used for two purposes. While the primary use for optimization of the website is mainly neutral for the user, the secondary use for advertisement purposes can cause actual negative effects. While in case of Google Analytics it is not known if the collected data is used for obvious harming methods like dynamic pricing [3] in Europe, behavioral information used for personalized advertisement can be used for influencing the decision of the user in a way that might not be in his favor [66; 40; 50]. Subjective negative consequences are mainly caused by concerns for (future) not known use of personal information, as well as the loss of control. The peculiarity of those concerns is influenced by the character of the data-subject itself but can also be affected by other factors that shape the expectation about the processing. Those include for example the amount of information accessible and comprehensible about the processing [62].

Furthermore, the description of the so-called privacy paradox showed, that privacy is treated by individuals not as something absolute but in a situational way. Depending on the expected return, individuals are willing to treat their privacy (in form of information disclosure) as a commodity [22].

3.3 Conclusion and method of further analysis

The prior section showed that negative impacts on the user's privacy are dependent on the subjective and objective consequences through the use of the collected data. It also showed that privacy can be interpreted as a commodity and thus can be subjected to economic principles. It can be concluded that the data collection qualifies as an externality because the website-owner has no incentive to consider the negative consequences for the user within his consumption-decision. For a market solution to be successful by negotiating, the requirements stated in section 2.2 apply. There must be legal as well as technical means to control or exclude the collection/ use of personal data. There must not be information asymmetries, thus every involved party must know the actual effect the collection of data has. This means for users that they must be aware of the objective and subjective consequences which affect his or her privacy. Lastly, the transaction costs must be sufficiently low, which requires adequate means of negotiation.

4 Potential of the data protection framework

4.1 Overview over existing law

The use of cookies, and especially the question if this action is required to get consent by the user, is one of most discussed topics within data protection law. The action of storing or reading out an Information (like a cookie ID) from the device of the end-user is addressed by Art. 8 of the ePrivacy Directive (2002/58/EC) [17]. Therefore, the end-user must give his or her consent to his action. Exceptions apply only if the processing is done for sole purposes of transmission, or the access is necessary to provide a service requested by the user. The consent must be given in a clear and informed way. If the usage of cookies for the purpose of general web-analysis requires user consent or if this

application qualifies as necessary to provide the service, is subject to ongoing legal discussion [59]. However, for further usage of the data for advertisement purposes, the jurisdiction clearly formulates the requirement for consent [9].

The further processing of the data is addressed by the General Data Protection Regulation (EU) 2016/679 (GDPR) [18]. The GDPR generally only allows the processing of personal data under the condition that there is a legal basis for this processing. The most important legal bases for processing are Art. 6 (for the processing of general personal information) and Art. 9 GDPR (for special categories of personal data). Relevant legal basis for the application of web-analytic tools is Art. 6 (1) (a) and (f) GDPR. The first options allow the processing if the data subject has given its consent while the second option requires a legitimate interest for the purpose of processing if those interests are not overridden by fundamental rights or freedoms of the data subject. Conditions for consent are stated in Art. 7 GDPR which generally requires the consent to be clearly given by the data subject in an informed way.

As many providers of web-analytic tools are American companies, the transmission of personal data must also comply with the requirements concerning transfer to third countries, which are set in Art. 44 – 50 GDPR. Those requirements generally want to prevent, that data is transferred into legal spaces, where the level of protection of personal data is significantly lower than within the EU [67]. In the aftermath of the Schrems II verdict by the European Court of Justice [13], the lawfulness transfer, especially to the US, has gotten significantly harder. The Reason is that before the Schrems II verdict, most of the transfer to the US was legally based on the so-called privacy shield. If the data importer was certified under the privacy shield, the European authorities generally acknowledged the lawfulness of the transfer. The European Court of Justice however judged that the requirements of the privacy shield certification do not ensure a level of data protection that is adequate to the GDPR. In the aftermath of the verdict, transfers of personal data must rely on another legal basis. Another possible legal basis for such transfer is again the consent of the user, as set in Art. 49 subparagraph 1 number a GDPR. In this case, the user must be informed about the risk the transfer inhibits. Legal discussions especially revolve around the question whether a procession that physically takes place within the EU by an American company, in which case the possibility of a transfer to the US or the access of US-American authorities cannot be excluded, would be lawful or not [60]. Further discussions revolve around the possibility of a transfer based on so-called standard contractual clauses (SCC). Also, the regular use of user consent as a legal basis for transferring is doubted by some authorities and legal scholars who argue, that the provisions of Art. 49 subparagraph 1 GDPR are formulated for single exceptional situations [57]. As the principle of "notification and consent" is the same as for the general processing, the regulations for third country transfer are not subject to deeper analysis in this paper.

4.2 Technological market aspects

Regulation and technology influence each other. Since regulation can indirectly (and most of the time explicitly) follow the goal of shaping or controlling the form of technology and markets, it can only be applied to existing technological situations. The scope is not only limited to the will of the regulator but also to the existing technological possibilities. Before going into the deeper analysis of the regulatory framework, this chapter wants to examine, if the requirements stated in section 3.3 are possible to achieve from a technological (and market) point of view in case of using tools for web-analysis.

Transaction costs can be significantly lowered as the cost for communication itself are decreased by technology and automatization enables the standardization of repeated negotiations. Within the use of web-analytic tools, this can be seen through the creation of the cookie-banner, which allows for a comparable simple negotiation medium. If this decrease of transaction cost is sufficient, is part of the further, more detailed discussion in section 4.5, because the actual implementation is influenced by regulatory means. However, the technical infrastructure is generally able to provide means for low transaction cost.

Furthermore, the creation of property or disposal rights, as well as the exclusion is technically also possible. As the use of web- analytic tools is not a technical obligatory requirement for operating most websites, the data collections

can technically be abandoned. Also, the enforcement of those rights can be technically realized to an extent. Technical standards like the "do not track" option when entering a website are established since 2012 and solutions for consent management have developed since [42]. However, technical enforcement only works to the extent that the data collecting party acts as agreed within the standards. Also, there are technical means for the user to prevent data collection, such as browser configurations or dedicated browser extensions. Those are generally effective, as long as the tracking is not realized by special techniques to circumvent this (e.g. through techniques like browser-fingerprinting) [49].

The market situation generally allows transaction to occur. However, the market for online advertisement might be vulnerable to monopolies, which could negatively affect an equal power distribution in negotiation [44]. This paper wants to focus on the effect of data protection laws. Antitrust aspects are therefore not further considered. However deeper research in this area can lead to further insights.

4.3 Assignment of right of disposal through data protection regulation

This section examines if the current regulatory framework allows for an assignment of rights of disposal for data. The first section looks at the general legal possibility for the right-assignment while the second part considers the possibility of the actual practical enforcement of those rights.

4.3.1 General possibility to assign rights of disposal.

This section is dedicated to examine how the right of disposal are realized through data protection regulation and if this method enables internalization.

Privacy is legislated as a fundamental right of the data subject in Art. 8 CFR. This high valuation as a fundamental right already makes it impossible within the legal system to subject the processing of personal to a fully *laissez-faire* market situation. Situations as described in the coase-theorem in which the damaged party pays money to the damager for omission, would violate principles of fundamental rights. Therefore, fundamental rights are granted to everyone and not only to those who are able to give the economic means to obtain them [52]. Even though fundamental rights are primarily rights to protect the individuals against misappropriated interventions of the state, the state also has the obligation to set a legal framework that also protects the individual from violations from third parties (theory of indirect third-party effect) [20]. This however does not mean that the processing of personal data per se must be prohibited without permission of the data subject. The data subject only has the right that its privacy is not interfered within an unappropriated way.

Applied to the subject of data collection through web-analytic tools, the fundamental rights character of privacy is considered within the secondary law by generally forbidding the data processing if there is not an appropriate reason or the user's consent (see section 4.1). Within this context, the law basically results in giving the data subject the right for disposal. This applies as well to the access to end-user device for cookie use, as well as for the data processing itself [6]. The ePrivacy Directive (2002/58/EC) gives fully the right to decide over the access to the device to its user, while only formulating exceptions for technical necessity without or with only minor impact on the user. While the use of web-analytic tools does not qualify as a technical necessity, in this context the user is fully in control.

Art. 6 (1) (f) the GDPR allows theoretically a form of "fair use" of personal data. If the rights and freedoms of the data subject are not negatively substantially impacted and the processer on the other side has a legitimate interest, the processing of the data would be allowed. This can be seen as some form of economical balance of interests. If the impact on the privacy of the user is not too high and the processor has a legitimate interest, which can be an economic benefit, this would effectively give the data-processer the initial power about the question whether a data collection is

allowed. This position initially was promoted by operators or web-analytic tools since it naturally fits their interests. Since then, the jurisdiction clarified, that data collection of user behavior to use for advertisement purposes, is not a legitimate interest [14]. This clarified legal uncertainty which existed before. Hence the processing is also dependent on the user consent according to Art. 6 (1) (a) GDPR, which effectively gives the user the power to decide whether such processing is executed or not. Same thing must be said about the transfer to a third country, which is dependent on the user consent according to Art. 49 (1) GDPR.

Within the current legislative framework, the initial right for disposal are clearly assigned to the data subject. As the processing is not entirely prohibited, but dependent on the consent of the user, the user is theoretically in charge to decide in which situation he or she gives his consent. By this, he or she can exclude other parties from processing his personal data, but the ability to give consent does not generally prohibit the processing.

Furthermore, the data subject gives his consent for specified processing purposes. Therefore, once collected personal data cannot be freely used or transferred willingly by the data-controller. This way, the data-subject theoretically is able to assess the consequences on his privacy by the time the transaction is made. Theoretically, there is the legal possibility to use personal data for other purposes than those which were the reason for the initial data collection with Art. 6 (4) GDPR. However, this applies to purposes which were not known by the time of the original collection, respectively by the time the original consent was given [58]. Therefore, in case of the collection through using web-analysis this norm cannot be applied because the further use of data for advertisement purposes is initially intended.

In conclusion, in theory the data subject is given the means to control over the rights of disposal of its personal data and hence is able to trade it as a commodity.

4.3.2 *Effectiveness of the right assignment.*

At first sight, as the user has control over the initial rights for disposal, he also seems to have the power about the initiative in the negotiation. However, in case of the use of web-analysis tools, the theory only transfers into practical experience up to a certain extent. When a user enters a website that uses web-analysis tools, it is on behalf of the website-owner to obtain the user's consent if they want to start the data-collection. The actual technical implication, how the consent is obtained (therefore the design of the so called "Cookie-Banner"), lies within the power of the website-owner. The user may be in power of the legal initiative, but the website-owner is in power about the practical process of the negotiation. This includes the actual negotiation terms (e.g. if the user is able to enter a website without giving his or her consent, if the is able to give his or her consent to specific purposes or for transfers to specific marketing providers etc.), but also about the interpretation if consent is given by a certain action. It is within the scope of the website-owner to pre-formulate a consent statement and the user is only able to approve or disapprove, mostly in a binary way. Even if there are ways to modify the terms of consent, the decision to which extent it is technological possible, is done by the website-owner.

This problem is also considered within the legal framework. Both, the GDPR and the ePrivacy Directive (2002/58/EC) formulate requirements for a valid consent. The GDPR formulates those requirements in Art. 7 GDPR. The ePrivacy Directive refers to the requirements for consent to the precursor directive of the GDPR [19], which is generally interpreted by the jurisdiction, that the norms of the GDPR apply nowadays. Generally, the interpretation if consent is given by the data subject must consider the "recipient horizon" of the data subject, as Art. 4 (11) GDPR defines consent as the freely given, specific, informed and unambiguous indication of the data subject's will. This means that the data subject objectively has to be aware, that the execution of a certain action results in giving consent. The GDPR also considers this by formulating the general principles of fairness and transparency for processing personal data in Art. 5 (1) (b) GDPR. Also Art. 7 (2) GDPR formulates the requirement to clearly distinguish single processing matters, in form of clear and plain language. Further, the responsibility to prove that a legit consent is

given, is assigned to the controller by Art. 7 (1) GDPR in connection with the general principle of accountability for the data controller in Art. 5 (2) GDPR. The theoretical result should be that no actions of the user are interpreted as consent, even if this is not the real will or interest of the user.

All this should theoretically give the user the power to enforce his or her rights of disposal in a way that fits his or her preferences and interests. However, practical applications showed that the legal requirements are formulated in a rather general unspecific way, which encouraged data-controllers to creative ways to interpret the concept of consent. There is a general trend to be seen in the practical implementations of the obtainment of consent, in which website-owners apply the most open possible interpretation of user actions as consent, if the jurisdiction does not explicitly rule certain designs as not compliant [63]. An example of that were websites that used consent-banners which used checkboxes that were checked by default but required a klick by the user to accept. This specific design was out ruled by the verdict ECLI:EU:C:2019:801 [14].

It can be seen that the general requirements by the law are slow but steadily specified by the jurisdiction. But there still exists a wide variety of methods to obtain consent by the user, that use behavioral patterns to obtain consent by the user against his original intention or interest [36]. Even though the use of so-called “dark patterns” is generally not compliant with the legal requirements [43], the formulation of the norms on a high abstraction-level and the slowness of the legal recourse led to a deficit of enforcement. A project of the data protection activist Max Schrems, who automated a process of detecting non-compliant “Cookie-Banner”, and reporting those to the responsible data protection authorities [47; 63], support the assumption, that the actual process of the obtainment of consent, is still highly against the favors of the user.

As a result, even if the user theoretically obtains the initial rights of disposal, he will be hindered to enforce those in a way that is effective.

4.4 Information asymmetries

As explained in section 3.3, a further requirement for successful integration of externalities is the non-existence of information asymmetries. Generally, the data-controller is in favor about information about the processing. He or she is the one who implements the web-analytic tool and decides which data is being collected on his website and transferred to the provider. He or she holds the power for the technical implementations and conventionalizes the use of certain “tracking-events”, thus the data points that are to be recorded. However, when entering a website, the user is generally not doing it with the intention to get tracked, which initially makes him or her the uninformed party within the negotiation [45]. One could argue, that the user should have a general expectation for this to happen, as this is common practice within the internet-economy but the details like the exact scope, the purposes as well as which third parties are involved, cannot exactly be known by the user [64]. However, the overall scope is relevant for the user to estimate the impact on his or her privacy and to come up with a decision that fits his or her economic preferences. As a result, the user has to put effort into informing himself with the means the website-owner offers.

This natural information asymmetry in favor of the data controller is also addressed by the legal framework. As the ePrivacy Directive (2002/58/EC) within its wording requires, the consent is to be given under the condition that the user has been provided “with clear and comprehensive information, in accordance with Directive 95/46/EC [(precursor directive to the GDPR)], inter alia, about the purposes of the processing”. One aspect of this information is that the user must know to which circumstances he gives his consent, otherwise his action cannot qualify as consent (as explained in the prior section). On the other side, the information about the scope and purposes also serves as general information about the processing scenario. The GDPR formulates further information duties in Art. 13 GDPR. Therefore, the controller must provide information among others about the purpose of the processing, the legal basis for the processing, recipients of the processed data, storage periods as well as his rights as a data subject. This

information should put the data subject into a position to comprehend the actual scope of the processing of his personal data. Also, especially the information about his rights as a data subject should inform him about the possibilities to act out his rights of disposal [56].

The legal framework contains aspects that clearly follow the intention or could effectively promote the user as a market actor on par and eliminate information asymmetries. But as assessed in the prior section, the practical implementation leaves doubts whether the intentions of the legal framework effectively transfer into real life.

First, it seems questionable that the user can fully assess the scope of the processing of his personal data, even with the provided information. Within the typical scenario, the user visits a website without the intention to start a negotiation. The application of the use of web-analysis tool itself is multilayered and complex: the user has to give a multi-purpose consent which addresses the access to his device (use of cookies), the processing for various purposes which are executed by different controllers (hence a transfer to a party that is not the one the user interacts with happens), as well as a transfer to a third country, which includes a different risk in itself [36]. Even though the controller is obligated to provide information in a form that is comprehensible for the data-subject, this legal requirement leaves vast room for interpretation. As it is the duty of the data controller, who holds the information monopoly about the processing at the beginning, there are not any incentive for him to give quality information to the data subject if he just complies with the law.

An example of this can already be seen in the formulation of consent statements. As stated above, there are certain different processing parts that require consent. As this includes the consent to access the device of the user for use of cookies, most of the designs of the "cookie-banner" to obtain consent use terms like "we need your consent for the use of cookies" as a headline. Even though within the further formulation of the consent statement the other circumstances and purposes are explained, the impression is evoked, that the consent is primarily given for the use of cookies. The use of cookies as means or as technology itself is mostly privacy neutral. There are various purposes, which do not impact privacy but are necessary for technical reasons (e.g. session cookies for login). As for those kinds of purposes, consent is not needed. This fact must also be explained within the consent statement. The consent statement, therefore, first explains the use of the technical means and then describes the purpose. Then it is explained that those means are also used for other purposes that do not require consent. This way of formulating the consent statement seems to be unnecessarily complicated, especially as not the means (cookies) but the purpose (collection personal information for advertisement) is the privacy impacting issue [63]. But this way of formulating a consent statement does not only comply with the law but is fostered by Art. 5 (2) ePrivacy Directive (2002/58/EC), which requires consent for access to the user-device as means. This complicated formulation-method does not actively withhold information from the user, but willingly makes them harder to comprehend. It at least seems questionable, if a visitor of a website who is casually surfing the internet is able, to reasonably comprehend this information to make a rational market decision.

The highlighting of the consent for cookie-use as means is one of many examples of how consent and privacy statements can be formulated in a way that is not deceptive but however euphemizes the nature of the data processing. As the actual formulation is the task of the website-owner, since he is initially the informed party, the user is dependent on him to give the information in a comprehensible way. As the law adheres room for interpretation regarding the actual implementation, the legal framework does not seem to contain effective tools to dissolve information-asymmetries [36].

In conclusion, the data protection-framework only seems to be able to diminish information asymmetries to an extent (for a deeper analysis of data asymmetries concerning data-driven companies see van de Waerd [2020]).

4.5 Transaction costs

As argued in section 4.2 the technological environment of the internet generally allows negotiation in a semi-automated way. The website-owner, therefore, determines through his design of the "Cookie-Banner" a predefined set of negotiation terms, that are customizable to a limited extent, and have to be accepted (or declined by the user). The result of the negotiation is automatically processed by the website. Even if there might be an initial effort to design the "Cookie-Banner" and to implement its functionality, the marginal cost per negotiation seems to be neglectable on the side of the website-owner. The user, on the other side, has to interact with a "Cookie-Banner" on every website he visits. Surveys lead to the assumption, that this significantly affects the user in his internet-experience [10; 38]. There are technical solutions for facilitating repeated decisions for the user. These include browser-configurations (activate "Do-not-Track"-Mode), use of browser-extensions (generally regarded as adblockers) or the use of Personal Information Management Services (PIMS) [1]. As most users seem to see no or only limited benefit in being tracked, those tools are not used in a way to automate negotiation but to automate the denying of consent [15]. Further transaction costs can be seen in the effort to eliminate information asymmetries. Initially, the website-owner holds all the information about the processing that is subject to the negotiation. Even though the website-owner is legally required to give the user access to the information, e.g., in the form of data-protection statements, the user must put in the effort in reading those and comprehend this information, as described in section 4.4. Especially for internet-users with limited technical backgrounds, this effort can be imagined as enormous up to impossible. This argument is supported by studies that examine the length of data-protection statements of major internet-platforms [11; 5].

In conclusion, technical means are generally able to reduce transaction costs, but especially the efforts to diminish information-asymmetries make an effective negotiation unlikely. In theory, high transaction costs should lead to a situation, where the initial owner of the disposal-rights decides to not engage in the negotiation. This could also explain the use of intrusive design patterns for consent-banners, that force the user to interact with them while hiding the options to deny consent [63]. This way, the website-owner can manipulate the user to interact and consent, by artificially increasing the transaction cost of not engaging, even if this method is not compliant with the law.

5 Conclusion

The current regulatory framework does not seem to be fitted to internalize the costs of the website-user through means of negotiation. Data protection laws do not solve issues concerning the effectiveness of the assignment of disposal-rights as well as the elimination of information asymmetries. The main reason for this is because even if the initial disposal-right for personal data is assigned to the data subject, the factual power about the way a negotiation is engaged, as well as the obligation to provide the essential information, is held by the website-owner. As the main interest of the website-owner is to get the consent of the user, he or she is not incentivized to create an efficient negotiation situation. He is more incentivized to manipulate the user by withholding or euphemizing information and to increase the effort to deny consent, as long as he is just compliant with the law. Here he or she takes advantage of the abstract formulation of the law as well as slow enforcement methods. The result is that the use of third-party web-analytic tools is higher than in the efficient market equilibrium.

Future jurisdiction as well as coming legislation, such as the E-Privacy directive, could improve the circumstances necessary for a successful negotiation, especially by out ruling misleading methods. However, it seems questionable, if information asymmetries can be resolved without causing too much effort for the website user.

REFERENCES

<bib id="bib1"><number>[1]</number> Serge Abiteboul, Benjamin André, and Daniel Kaplan. 2015. Managing your digital life. *Commun. ACM* 58, 5 (May 2015), 32–35. DOI:https://doi.org/10.1145/2670528</bib>
<bib id="bib2"><number>[2]</number> Alessandro Acquisti, Curtis Taylor and Liad Wagman. 2016. The economics of privacy. *Journal of economic Literature* 54, 2(2016), 442-492.</bib>
<bib id="bib3"><number>[3]</number> Alessandro Acquisti and Hal Varian. 2004. Conditioning Prices on Purchase History. *Marketing Science* 24, 2 (February 2004), 367-381.</bib>
<bib id="bib4"><number>[4]</number> Alphabet. 2021. Google Code of Conduct. (September 2020). Retrieved February 3, 2022 from https://abc.xyz/investor/other/google-code-of-conduct/</bib>

<bib id="bib5"><number>[5]</number> Ryan Amos, Gunes Acar, Elena Lucherini, Mihir Kshirsagar, Arvind Narayanan, and Jonathan Mayer. 2021. Privacy Policies over Time: Curation and Analysis of a Million-Document Dataset. *Proceedings of the Web Conference 2021*. Association for Computing Machinery, New York, NY, USA, 2165–2176. DOI:https://doi.org/10.1145/3442381.3450048</bib>
<bib id="bib6"><number>[6]</number> Art. 29 Data Protection Working Party. 2012. Opinion 04/2012 on Cookie Consent Exemption. Retrieved Ferbruary 7, 2022 from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf</bib>
<bib id="bib7"><number>[7]</number> Andy H. Barnett. 1980. The Pigouvian tax rule under monopoly. *The American Economic Review* 70, 5 (1980), 1037-1041.</bib>
<bib id="bib8"><number>[8]</number> Mathias Brandt. 2017. Sie wissen, was du letzten Sommer geklickt hast [Digitales Bild]. (December 2017). Retrieved 27. Januar 27, 2022 from https://de.statista.com/infografik/12252/tracking-reichweite-von-internet-unternehmen/</bib>
<bib id="bib9"><number>[9]</number> Bundesgerichtshof, Judgement I ZR 7/16, 28.05.2020.</bib>
<bib id="bib10"><number>[10]</number> Corina Cara, Lorena Florentina Dumitraşciuc and Alexandru Ioan Cuza. 2021. GDPR consent pop-ups. How are we thinking about them? An Elaboration Likelihood perspective. *Journal of International Business and Management* 4, 1 (2021), 01-10.</bib>
<bib id="bib11"><number>[11]</number> Adam S. Chilton and Omri Ben-Shahar. Simplification of Privacy Disclosures: An Experimental Test. *Coase-Sandor Working Paper Series in Law and Economics* 737, (2016). </bib>
<bib id="bib12"><number>[12]</number> Ronald Harry Coase. 1960. The Problem of Social Cost. *The Journal of Law & Economics* 56, 4 (November 2013), 837-877.</bib>
<bib id="bib13"><number>[13]</number> Court of Justice of the European Union, Judgment ECLI:EU:C:2020:559I, 16.07.2020.</bib>
<bib id="bib14"><number>[14]</number> Court of Justice of the European Union, Judgment ECLI:EU:C:2019:801, 01.10.2019.</bib>
<bib id="bib15"><number>[15]</number> Deloitte. 2020. Cookie Benchmark study. (April 2020). Retrieved February 7 from https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-cookie-benchmark-study.pdf</bib>
<bib id="bib16"><number>[16]</number> Econsultancy. 2012. Online Measurement and Strategy Report 2012 (Juli 2012). Retrieved February 3, 2022 from https://de.statista.com/statistik/daten/studie/235496/umfrage/anteil-der-premium-nutzer-von-google-analytics/</bib>
<bib id="bib17"><number>[17]</number> The European Parliament and the Council of the European Union. 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Official Journal of the European Communities.</bib>
<bib id="bib18"><number>[18]</number> The European Parliament and the Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119/1.</bib>
<bib id="bib19"><number>[19]</number> The European Parliament and the Council of the European Union. 1995. Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Communities.</bib>
<bib id="bib20"><number>[20]</number> Eric Engle. 2009. The Third Party Effect of Fundamental Rights (Drittwirkung). *Hanse Law Review* 5, 2 (2009) 165-173.</bib>
<bib id="bib21"><number>[21]</number> Michael Fritsch. 2011. *Marktversagen und Wirtschaftspolitik* (8th. ed.). Franz Vahlen, München München.</bib>
<bib id="bib22"><number>[22]</number> Nina Gerber, Paul Gerber an Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77, (August 2018), 226-261 https://doi.org/10.1016/j.cose.2018.04.002</bib>
<bib id="bib23"><number>[23]</number> Google. About Analytics. Retrieved February 3, 2022 from https://marketingplatform.google.com/intl/de/about/analytics/</bib>
<bib id="bib24"><number>[24]</number> Google. About Analytic s- Features. Retrieved February 3, 2022 from https://marketingplatform.google.com/intl/de/about/analytics/features/</bib>
<bib id="bib25"><number>[25]</number> Google. Google Analytics Cookie Usage on Websites. Retrieved February 3, 2022 from https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage</bib>
<bib id="bib26"><number>[26]</number> Google. Create and manage Custom Reports. Retrieved February 3, 2022 from https://support.google.com/analytics/answer/1151300?hl=en#zippy=%2Cin-this-article</bib>
<bib id="bib27"><number>[27]</number> Google. Data sharing settings. Retrieved February 3, 2022 from https://support.google.com/analytics/answer/1011397?hl=en#zippy=%2Cthemen-in-diesem-artikel%2Cin-this-article</bib>
<bib id="bib28"><number>[28]</number> Google. Demografische Merkmale und Interessen. Retrieved February 3, 2022 from https://support.google.com/analytics/answer/2799357?hl=de#zippy=%2Cthemen-in-diesem-artikel</bib>
<bib id="bib29"><number>[29]</number> Google. Universal Tracking Events. Retrieved February 3, 2022 from https://support.google.com/tagmanager/answer/6106716?hl=en</bib>
<bib id="bib30"><number>[30]</number> Google. [GA4] Set up and manage conversion events. Retrieved February 3, 2022 from https://support.google.com/analytics/answer/9267568?hl=en#zippy=%2Cin-this-article</bib>
<bib id="bib31"><number>[31]</number> Google. 2021. Datenverarbeitungsbedingungen für Google Ads. (September 2021). Retrieved February 3, 2022 from https://business.safety.google/adsprocessorterms/ </bib>
<bib id="bib32"><number>[32]</number> Google. 2021. Google Analytics Terms of Service. (June 2019). Retrieved February 3, 2022 from https://marketingplatform.google.com/about/analytics/terms/us/</bib>
<bib id="bib33"><number>[33]</number> N. Gregory Mankiw and Mark P.Taylor. 2021. *Grundzüge der Volkswirtschaftslehre* (8th. ed.). Schäffer-Poeschel, Stuttgart.</bib>
<bib id="bib34"><number>[34]</number> Paul Graß, Hanna Schraffenberger, Frederik Zuiderveen Borgesius and Moniek Buijzen. 2021. Dark and bright patterns in cookie-consent requests. *Journal of Digital Social Research* 3, (February 2021), 1-38.</bib>
<bib id="bib35"><number>[35]</number> Joerg Heidrich and Michael Koch. 2020. Die Nutzer im Netz zwischen Einfluss und Ohnmacht. *MMR* 9 (September 2020), 581-586.</bib>
<bib id="bib36"><number>[36]</number> Philip Hausner and Michael Gertz 2021. Dark Patterns in the Interaction with Cookie Banners. arXiv preprint arXiv:2103.14956. Retrieved from https://arxiv.org/abs/2103.14956</bib>
<bib id="bib37"><number>[37]</number> Jean-François Hennart. 1986. What Is Internalization? *Weltwirtschaftliches Archiv* 122, 4 (1986), 791–804.</bib>
<bib id="bib38"><number>[38]</number> Maximilian Hils, Daniel W Woods and Rainer Böhme, Rainer. 2021. Privacy Preference Signals: Past, Present and Future. *Proceedings on Privacy Enhancing Technologies*. 2021. 249-269.</bib>

<bib id="bib39"><number>[39]</number> Thomas Hoeren and Philip Bitter. 2019 (Re)Strucutring Data Law: Approaches to Data Property. [] Bergener/Räckers/Stein (Ed.), *The Art of Structuring*. Springer, Berlin. 297-305.</bib>
<bib id="bib40"><number>[40]</number> Kai-Lung Hui and IPL Png. 2006. The Economics of Privacy. Terrence Hendershott (Ed*.), Handbook in Information Systems, Vol. 1*, Elsevier, B.V.</bib>
<bib id="bib41"><number>[41]</number> Tim Jülicher. 2015. Daten in der Cloud im Insolvenzfall – Ein internationaler Überblick. *Kommunikation und Recht (K&R)* 8 (August 2015), 448-452.</bib>
<bib id="bib42"><number>[42]</number> Irene Kamara, Eleni Kosta, Do Not Track initiatives: regaining the lost user control, *International Data Privacy Law* 6, 4 (April 2016), 276-290.</bib>
<bib id="bib43"><number>[43]</number> M. R. Leiser and Mirelle M. Cuarana. 2021. Dark Patterns: Light tob e Found in Europes Consumer Protection Regime. *EuCML* 6 (2021) 237-252.</bib>
<bib id="bib44"><number>[44]</number> Duncan McCann, Will Stronge and Phil Jones. 2021. The Future of online Advertising – Exploring the impacts of surveillance-based advertising, current trends in adtech and the challenges and opportunities oft a total ban on the use of personal data. (October 2021). Retrieved February 7, 2022 from https://digitalcourage.de/sites/default/files/2021-10/McCann%2C%20Stronge%2C%20Jones%20%282021%29%20-%20The%20Future%20of%20Online%20Advertising.pdf</bib>
<bib id="bib45"><number>[45]</number> Aleecia McDonald and Jon M. Peha. 2011. Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature. (September 25, 2011). *TPRC*, (September 2011).</bib>
<bib id="bib46"><number>[46]</number> Eli M. Noam and Everett C. Parker. 1994. Privacy in Telecommunications: Markets, Rights and Regulations. Office of Communication, United Church of Christ.</bib>
<bib id="bib47"><number>[47]</number> Noyb. 2021. noyb setzt dem Cookie-Banner-Wahnsinn ein Ende. (May 31, 2021). Retrieved February 7, 2022 from https://noyb.eu/de/noyb-setzt-dem-cookie-banner-wahnsinn-ein-ende </bib>
<bib id="bib48"><number>[48]</number> Boris P. Paal and Moritz Hennemann. 2018. Big Data as an Asset. Retrieved February 3, 2022 from https://www.abida.de/sites/default/files/Gutachten_ABIDA_Big_Data_as_an_Asset.pdf. </bib>
<bib id="bib49"><number>[49]</number> Emmanouil Papadogiannakis, Panagiotis Papadopoulos, Nicolas Kourtellis, and Evangelos P. Markatos. 2021. User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users. Proceedings of the Web Conference 2021. Association for Computing Machinery, New York, NY, USA, 2130–2141. DOI:https://doi.org/10.1145/3442381.3450056</bib>
<bib id="bib50"><number>[50]</number> David J Park. 2017. Individualization, information asymmetry, and exploitation in the advertiser-driven digital era. *The Political Economy of Communication* 5, 2(2017), 22-44.</bib>
<bib id="bib51"><number>[51]</number> Paul A. Pavlou. 2011. State of the information privacy literature: where are we now and where should we go? *MIS Quarterly* 35, 4 (December 2011), 977-988.</bib>
<bib id="bib52"><number>[52]</number> Denise Quintel and Robert Wilson. 2020. Analytics and privacy. *Information Technology and Libraries* 39, 3 (2020).</bib>
<bib id="bib53"><number>[53]</number> Eric A. Posner. 2008. Human welfare, not human rights. *Columbia. Law Review* 108, (2008), 1758-1801.</bib>
<bib id="bib54"><number>[54]</number> Sunita Rai. 2019. Matomo vs. Google Analytics – Which is a Better Web Analytics Tool? (September 2019). Retrieved February 7, 2022 from https://www.monsterinsights.com/matomo-vs-google-analytics/</bib>
<bib id="bib55"><number>[55]</number> Allen Randall. 1983. The Problem of Market Failure. *Natural Resources Journal* 23, 1 (1983): 131–48.</bib>
<bib id="bib56"><number>[56]</number> Christoph Reich. 2018. Überblick über Betroffenenrechte nach der Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (neu). *Verbraucher und Recht*, 8 (August 2018), 293-297.</bib>
<bib id="bib57"><number>[57]</number> Barbara Sandfuchs. 2021. The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II. *GRUR Int*. 70, 3 (March 2021), 245-249.</bib>
<bib id="bib58"><number>[58]</number> Joseph Savirimuthu. 2021 Lawfulness of Pre-formulated Declarations of Consent. *EuCML*, 4 (2021), 169-172.</bib>
<bib id="bib59"><number>[59]</number> Pascal Schumacher, Lennart Sydow and Max von Schönfeld. 2021. Cookie Compliance, quo vadis? *MMR*, 8 (August 2021), 603-609.</bib>
<bib id="bib60"><number>[60]</number> Rolf Schwartmann und Lucia Burkhardt. 2021. Schrems II" als Sackgasse für die Datenwirtschaft? *Zeitschrift für Datenschutz*, 5(May 2021), 235-257.</bib>
<bib id="bib61"><number>[61]</number> Jen Slemp. 2019. Is Google Analytics 360 Worth the Price Tag?. Retrieved February 7, 2022 from https://www.thirdandgrove.com/insights/is-google-analytics-360-worth-price-tag/</bib>
<bib id="bib62"><number>[62]</number> H. Jeff Smith, Tamara Dinev, Heng Xu. 2011. Information Priviacy Research: an interdisciplinary review. *MIS Quarterly* 35, 4 (December 2011), 989-1015.</bib>
<bib id="bib63"><number>[63]</number> Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*, November 11–15, 2019, London, United Kingdom. ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3319535.3354212</bib>
<bib id="bib64"><number>[64]</number> Peter J. van de Waerdt. 2020. Information asymmetries: recognizing the limits of the GDPR on the data-driven market. *Computer Law & Security Review* 38, (September 2020).</bib>
<bib id="bib65"><number>[65]</number> Arild Vatn and Daniel W. Bromley. 1997. Externalities — A market model failure. *Environmental and Resource Economics* 9, 2 (1997), 135–151. https://doi.org/10.1007/BF02441375</bib>
<bib id="bib66"><number>[66]</number> Sandra Wachter. 2021. Affinity Profiling and Discrimination by Association in Online Behavioural Advertising. *Berkeley Technology Law Journal* 35, 2 (2021), 369–430.</bib>
<bib id="bib67"><number>[67]</number> Julian Wagner. 2018. The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? *International Data Privacy Law.</bib>*
<bib id="bib68"><number>[68]</number> Web Technology Surveys. Usage statistics and market share of Google Analytics for websites Retrieved February 3,2022 from https://w3techs.com/technologies/details/ta-googleanalytics</bib>