ISSN 2281-5147

WHY YOUR DATA IS NOT YOUR PROPERTY (AND WHY YOU STILL END UP PAYING WITH IT)

Onntje Hinrichs*

Abstract

This essay explores three interrelated topics that reveal tensions in the European approach towards the regulation of the data economy: (i) data as property (ii) data and fundamental rights, and (iii) data as payment. By retracing how scholars and policy makers have attempted to find an appropriate regulatory framework for the data economy, this essay shows that up to this day, contradictions in the EU's approach to the data economy persist and become evident in our everyday lives online. Despite not owning our data, we pay for digital content and services with it. This essay clarifies this paradox and its role in ongoing legal battles between the large corporations, civil society and the EU.

Table of Contents

* Onntje Hinrichs is a PhD Researcher at the Research Group on Law, Science, Technology and Society (LSTS), Vrije Universiteit Brussel (VUB) and a Marie-Sklodowska Curie Action Fellow in the Legality Attentive Data Scientists project. His research explores emerging forms of data governance in EU law and how consumer law shapes the regulation of data. E-mail address: onntje.marten.hinrichs@vub.be
This work is supported by the European Union's funded project Legality Attentive Data Scientists (LeADS) under Grant Agreement no. 956562

ISSN 2281-5147

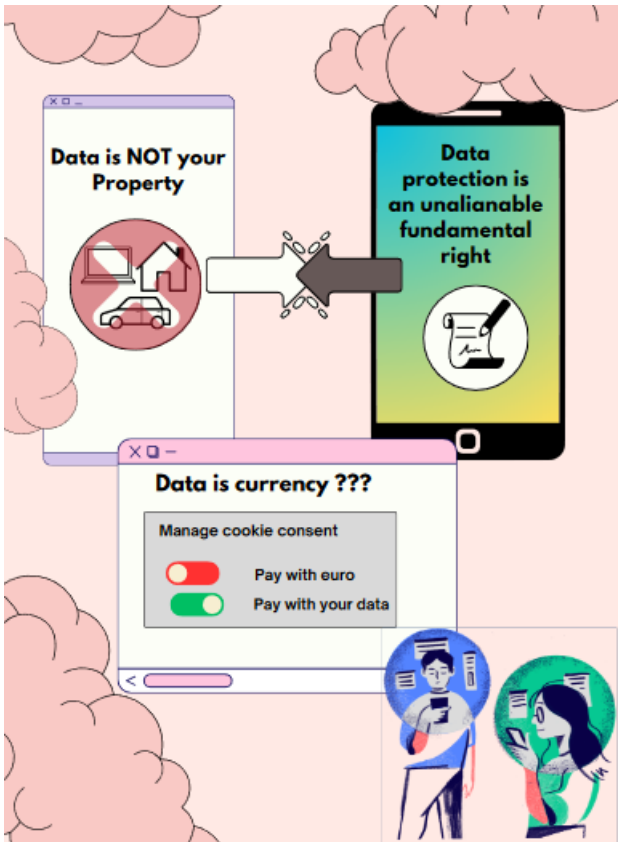
Keywords

Data Protection – Data Economy – Data Property – Consumer Protection – Pay-Or-Consent

ISSN 2281-5147

1. Introduction

If data is considered as the new oil, shouldn't we as consumers somehow benefit monetarily from allowing others to harvest 'our' personal information? Put more polemically, if our shopping habits online are the new oil fields of the 21st century, does that mean we will all become rich?



We do not 'own' our data. It is protected as a fundamental right instead – but we experience online that in practice data constitutes a form of payment. This essay explains this paradox and the challenges it creates.

The last question is evidently polemic as it simplifies and caricatures the metaphors of 'data as the new oil' or 'data as the new gold to be mined' which have increasingly been employed by businesses and policy makers to highlight the importance of data for the information economy. Nevertheless, as is often the case with caricatures, they contain elements of truth and reflect important questions we as society have to deal with. Moreover, these topics are grounded in debates that have marked academic and policy discourse over the past decades on how to regulate the data economy. This essay is structured around three interrelated topics that are still central to the regulation of the data economy: (i) **data as property**, (ii) **data and fundamental rights**, and finally (iii) **data as payment**.

The first section explains why 'our' data cannot be considered as our property – contrary to resources such as oil or precious metals such as gold. It outlines, how scholars and policy makers have debated whether introducing property rights in data could be a viable way for individuals to control and benefit economically from their data. Furthermore, it might facilitate the emergence of competitive data markets. The second section on data and fundamental rights, elaborates upon how 'our' data is currently protected within the legal data protection framework of the EU. It explains

ISSN 2281-5147

why the European approach has been described as incompatible with the idea of 'data property' (Mayer-Schönberger, 2010).

Whereas 'property' rights might typically enable us to sell, destroy or rent objects we own, fundamental rights are for evident reasons very different. We should not be able to transform our fundamental right into a commodity that can be bought and sold on a market. It should be impossible to put a price tag on human dignity which is thus described as an unalienable fundamental right. However, if data property stands in direct opposition to the fundamental right to data protection, there should be no necessity to deal with the last topic of this essay: data as payment. Counter-intuitively, however, this remains a highly contentious issue and the last section of this essay explains why. It exemplifies how seemingly trivial things such as cookie banners reflect complex legal questions to which thus far no conclusive answer exists. This essay clarifies this paradox and its role in ongoing legal battles between large corporations, civil society, and European Institutions.

2. Data as Property

In our everyday language, it has become perfectly normal to refer to 'our' data when we speak about the traces which we leave online, and which are used by companies for commercial purposes. For instance, whenever we visit online shops, our data is used to create profiles about our consumption habits. The objective: to show us other products and services which, based on the collected data, we might be interested in. When we speak about 'our' data, it expresses how we feel about information that relates to us. Since the traces which we leave when we browse the internet oftentimes reveal private and intimate information about us, such as our sexual orientation or political views when we 'like' certain content on social media, it makes sense to intuitively claim ownership over such data and to prevent others from using them. 'Our' data should belong to us. Such language thus reflects how the notion of ownership can be a psychological concept that expresses a sense of belonging. From a legal perspective, however, 'ownership' and 'property rights' denote something entirely different.

From a legal perspective, property rights do not come automatically into existence because of a felt claim over something. Instead, property rights have to be artificially

ISSN 2281-5147

created by the law. It is the law which exclusively defines what can and cannot be owned. It is the law which defines to what extent and under which conditions others can interfere with our property. Whereas a contract is only binding on the contracting parties, property rights can be enforced against everybody else. When you own a house, you can exclusively and selectively determine, who should be able to enter. You may decide to rent, to sell, or even destroy it. Your ownership thus lasts until you decide to end it. Deciding why certain things should (not) be treated as objects of property law, is thus a highly sensitive question as the rights conferred are far-reaching and are binding to others. Think again about the metaphor of owning a house. You can prevent people from entering your house. If they still enter against your will, you can call the police to enforce your rights.

Should data be considered as an object of property law? Should the law create new property rights that can be invoked between individuals and businesses with regard to data? Again counter-intuitively, this is not a new question but has been a hotly debated issue for several decades. Already in 1968, decades before the collection of data both online and offline has become ubiquitous, authors argued that the right we as individuals have over our personal information should be understood as a property right (Westin, 1968). Conceiving our personal information as property would give us control over our personal information. Just like property rights over tangible objects give us the possibility to exclude others from using them, property rights over (intangible) information should empower us to exclude others from using it without our permission.

This argument gained prominence with the growing importance of the internet during the 90s. Whilst our personal information was already being collected in the physical world, it still required comparably more effort. With the emerging architecture of digital cyberspaces, on the other hand, the collection of our personal information was becoming the new default. Data property was thus believed by many as a solution to empower us online with regard to our data (Lessig, 1999). Without our approval, companies would not be allowed to use any of our personal information. If, however, we wanted to sell our data to the highest bidder, a property rights regime would empower us to do so. Data property would thus not only be a useful instrument to protect citizens' data, but at the same time it would benefit the economy since it could

ISSN 2281-5147

facilitate the emergence of data markets and thus the availability of data for companies.

Today, however, we still have not created property rights for data. We might talk about 'our' data in everyday language, but this does not mean that 'your' data is 'your' property from a legal perspective. It expresses a felt entitlement over 'our' information, but it does not translate into corresponding legal property rights. Therefore, you do not own 'your' data in a similar way you own your car, laptop, or house. The reasons why we have not taken this path are many. Some relate to the traits of data (as a non-physical object, how do you transfer property rights from one person to another?), others to determining its value (what is the precise value of our data – can you ascribe monetary value to it in a similar way we do with physical objects?), and others to general societal objectives and how they can be best achieved through law (shouldn't information be 'free as the air we breathe' to foster culture and artistic expression or innovation?). Most importantly in Europe, however, the creation of property rights in data was believed to be diametrically opposed to the foundation of European data protection law: Data protection in Europe constitutes a fundamental right which is enshrined in article 8 of the Charter of Fundamental Rights of the European Union.

3. Data Protection as a Fundamental Right

Why is the conception of data protection as a fundamental right difficult to be reconciled with the creation of property rights in data? Rights that are characterized as being 'fundamental' denote core values of our European society. Whereas some of such rights, whether it is the fundamental right to data protection, freedom of expression, or freedom of assembly, can be limited under certain circumstances – their core is absolute. This implies furthermore, that they are not considered as simple commodities which can be bought and sold on the market. Considering data as property would, however, make it akin to any other object which companies can purchase from citizens or which citizens can sell to a price they deem appropriate. Within the European Union, it is therefore difficult, if not impossible, to conceive data as property since it might turn a fundamental right into a commodity that can be

ISSN 2281-5147

bought and sold on the market – it would put a price tag on the right to data protection.

If not through property rights that grant us ownership over our data, how does European data protection law intent to protect or empower us as citizens with regard to our personal information? Most famously, through the General Data Protection Regulation, short GDPR. Often criticized for the bureaucratic burdens which it would impose on any type of business, regardless of its size and field of activity, it is the GDPR that imposes constraints on what public bodies and businesses can and cannot do with our data. It is the GDPR which has been used to inflict heavy fines on some of the largest corporations for their violations of EU data protection law: 1.2 billion euro for Facebook, 746 million euro for Amazon, 345 million euro for TikTok[1] – the numbers constitute a powerful reflection of the 'value' which the law ascribes to the protection of our data.

The regime for fines which the GDPR created for breaches of European Data Protection law, should of course only constitute one of the last means to ensure that our data is protected. It would be preferrable if companies and public bodies only use our data in a way that is compliant with the GDPR. Over 88 pages, the GDPR outlines rules which any entity that processes personal data has to comply with. It creates a set of rights which should empower us as citizens over our data – such as the right to access or delete data which companies have collected about us. It creates a variety of obligations to empower citizens through information. Privacy notices are an example of this. Companies must be transparent about what they do with our data. The law wants to put us in the position to better understand what happens to our data and to act accordingly (De Hert & Gutwirth, 2009). Companies and public bodies, on the other hand, must show at all times that they comply with the GDPR. If they fail to do so, they can be held accountable, for instance, through the imposition of fines.

This regulatory regime thus forces entities that use our data to always have in mind the obligations of the GDPR whenever they use our data. For instance, the GDPR classifies certain types of information as 'sensitive data', such as data concerning our health, sexual orientation, or political opinion. Whenever such data is being used, the GDPR imposes much stricter use conditions – reflecting again the fundamental rights

[1] For an overview of fines under the GDPR see for example https://www.enforcementtracker.com/

ISSN 2281-5147

rationale of the GDPR. Finally, in all such cases, the processing of our data must be 'lawful'. What does 'lawful processing' of our data mean within the context of the GDPR? The GDPR creates six major justifications ('legal basis') which companies or public bodies must rely upon when they want to use our data. If they fail to do so, the use of our data would be illegal. For instance, in some cases our employers may have to report our data to social security or tax authorities. Since the law imposes this obligation on companies, the GDPR authorises the use of our data in such circumstances. One of the most (in)famous justifications companies can rely upon when they want to use our data is 'consent'. What does 'consent' under European data protection law mean?

The GDPR needs roughly 900 words, spread over different articles and recitals of the GDPR, to explain what 'legal' consent means. The European Data Protection Board, a body which consists of representatives from all national data protection authorities and which is tasked with giving guidance on the application and interpretation of European data protection law, has issued two guidelines on what consent is under the GDPR (both put together total roughly 60 pages or 35.000 words). The answer to 'what constitutes legal consent' under the GDPR therefore does not seem to be an easy one.

Put in GDPR terms, consent should be a freely given, specific, informed and unambiguous indication of our wishes. Can we 'freely consent' when our employer asks us if it can process our data? Probably not. The dependency inherent to an employer/employee relationship and the possible repercussions if we say 'no' to our employer might stop us from 'freely' consenting. Furthermore, we should always be given a genuine free choice – for instance, consent should not be tied to the provision of a service or the access to digital content. If you only get something you want if you must consent to the processing of your data, it is not really 'freely given'. Instead, it seems more akin to a sort of payment which you provide in return for something you want.

4. Data as Payment

The first two sections of this essay outlined how data is protected as a fundamental right in the EU and how it cannot be considered as our property. As outlined in the

ISSN 2281-5147

first part of this essay, the idea of creating 'property rights' in data was rejected since we should not be able to 'own' or 'sell' our data on the marketplace. The second part explained this particularity of the European approach by elaborating upon the fundamental rights rationale that underpins European data protection law. It intends to protect our data through a variety of rules created by the GDPR. If data is not property but protected as an unalienable fundamental right instead, can data constitute some form of digital payment?

Following this line of reasoning, the obvious answer should be clearly: no, it cannot.[2] This is further exemplified by the characterisation of 'consent' as 'freely given'. The GDPR understands consent to the use of data as something that is not conditional for subsequent access to digital content.

However, the reality for most of us is different when we try to access digital content or digital services. Whenever you visit the website of a news publisher to gain access to articles for 'free', you have probably encountered so called 'cookie-walls'. 'Cookie-walls' (see image in beginning of the article) provide visitors of a website with the following binary choice: if they want to access the digital content of the website, visitors either have to agree that the publisher can use their data (for instance for marketing purposes) or they have to pay for a subscription. However, if digital content can only be accessed in exchange either for data or for money it is easy to perceive our personal information as some form of alternative payment. Such an approach thus seems contrary to the perception of the right to data protection as an unalienable fundamental right. Are such practices contrary to European data protection law?

Again, one would expect a clear answer. If data must not be considered as something that can be bought and sold on the market (it cannot be considered as property) but is protected as an unalienable fundamental right, data should not be considered as

[2] See in that context also European Data Protection Supervisor (EDPS), 2017 Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. When the 2017 proposal for a Digital Content Directive intended to introduce the idea of data as counter-performance (meaning legally recognizing consumer data as a form of payment) the EDPS warned against any provision that would introduce the idea that people can pay with their data. For the EDPS it was clear that fundamental rights 'cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity'. In drastic words the EDPS observed how 'There might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation.'). When the final text of the Digital Content and Digital Services Directive was adopted two years later in 2019, it no longer described data as 'counter-performance' and highlighted how personal data could not be considered as a commodity.

ISSN 2281-5147

payment and such practices should not be allowed under European data protection law. However, the answers given by national data protection authorities differ. Some countries in the EU, thus seem to accept such business models. The European Data Protection Board, a group where members of all national data protection authorities meet, stated in 2020 that cookie walls which do not give consumers any other option apart from 'consenting' to the use of their data are contrary to data protection law. The French data protection authority in 2022, gave a more nuanced opinion. Cookie walls can be lawful, if they give consumers a real choice. This choice can consist of (i) either consenting to the use of our data or (ii) paying a *reasonable price* for accessing the digital content. What is a *reasonable price*? This would depend on each case.

Similarly, the Austrian data protection authority in 2023 argued how such cookie walls can be in accordance with data protection law. Consumers should have a certain degree of autonomy to decide what happens with their data (and thus chose if they want to pay for a service or consent to the processing of their data). Similarly to the French data protection authority, the Austrians highlighted that each solution would require a careful balancing of interests – the interests of us as consumers, but also the interests of companies who offer their services without monetary payment but in exchange for data. The Austrian authority was cautious in its approach because simply accepting any 'pay-or-consent' model would risk that low-income consumers in particular would always have to pay with their data since they cannot afford the 'pay' variant.

The cases from the French and Austrian data protection authorities both concerned cases where cookie walls were used by news publishers. In both cases the news publishers argued, how the collection of our personal information constituted a necessary counter-performance for their work – for example, journalistic articles. Since our information is subsequently being commercially exploited and monetised through the deployment of personalised advertisement, it enables publishers to finance their work and to provide us their content for 'free' – without obliging us to pay but to merely consent to the processing of our data. From a business perspective it thus equally is understandable how the processing of our personal information is an economic necessity for companies that provide digital content without monetary counter performance.

ISSN 2281-5147

'This Service is Free and will Always Remain Free'

One of the largest social media platforms advertised its services for years with the slogan 'Our services are free and will always remain free'. Beyond being a slogan to marketize its product, it also reflected a mentality online that every digital content, every digital service we use and consume is (and should be) available for free. Up to this day, some of the most used digital services, such as E-Mail or social media services, are provided in exchange for data and not for monetary payments.

Does the law challenge such business models? Think about the marketing slogan from a consumer protection perspective. Should such advertising be declared illegal because it makes a claim that is factually wrong and therefore misleading consumers? Are such services actually free? Do or do we not pay with our personal data? What this essay has tried to show is how complicated such a seemingly trivial question is. From a data protection perspective, the marketing slogan might be considered truthful. It is data protection law that insists on the fact how data is not a commodity (that cannot be propertized) and how we cannot pay with our data. When Facebook was brought to court over the legality of this marketing slogan, it used precisely this line of defence. It cited the European Data Protection Supervisor that data is not a commodity and that we as consumers would therefore of course not pay with our data for Facebook's service – hence their service could be marketed as being 'free'. This constituted of course a smart, but absurd, line of argumentation since it was one of the most infamous infringers of data protection law that relied on a European data protection institution to justify and defend the legality of its commercial practices. As one of the most profitable companies worldwide, Facebook certainly does not intend to donate its services to consumers.

More recently, Facebook, again, had to adapt its commercial practices to make them compliant with European law. As outlined during the second section of this essay, it needed a legal justification to ensure that it could use the data of its users in a lawful manner.[3] Facebook decided to rely on consent. It offered the following binary choice to consumers: either agree that we can use your data for targeted advertisement or

[3] See CJEU case C-252/21 Meta v Bundeskartellamt, [2023] ECLI:EU:C:2023:537. In this case which opposed Meta and the German competition authority, the European court clarified that Facebook needed consumer's consent if it wanted to use their data for its advertising business model and could not rely on, for instance, the legal basis of the GDPR where data processing is necessary for the performance of a contract. See e. g. paragraph 150 of the judgment.

ISSN 2281-5147

pay us a monthly subscription fee (at the time of writing of this article 9,99€/month). Put differently, either pay with your data or with your money.[4]

5. Conclusion

Your data is thus not your property, but (at the moment at least) you will still end up paying with data for services and digital content. This essay showed this unintuitive conclusion through three sections. First, it explained why data is not considered as property in the EU. You are not the owner of your data in a similar way you can be the owner of a house. Instead, our data is protected through the unalienable fundamental right to data protection. It showed how both concepts are fundamentally opposed. Whereas legal property rights enable us to buy and sell objects on the market, the fundamental right to data protection wants to precisely prevent that our data is transformed into a mere commodity. The third section showed, however, that in practice we do end up paying with our data for services. This becomes explicit when we are presented with the binary choice of either consenting to the processing of our data or paying with our money for a service. Here, data is transformed into an alternative means of payment.

At the same time, this essay showed that there is no obvious solution to this. The law still struggles with the precise classification of data. On the one hand it stresses the fact that data cannot be a commodity. On the other hand, it is obvious that economic value can be extracted from our data. When companies collect our data to commercially exploit it for marketing purposes, it oftentimes provides them with the necessary financial gains that enable them to provide their content or services for 'free'. Whereas we as consumers benefit financially from using many online services without having to pay with our money for them, the risk from fully accepting such business models is equally clear. It would ultimately risk turning the fundamental right to data protection into a commodity we have to pay for.

[4] (According to a CEO of the "Pay or Okay" provider, when faced with the choice of either consenting or paying 1,99€ for the use of online services, 99.9% of the users chose to 'pay' with their data. See 'noyb files GDPR complaint against Meta over "Pay or Okay" [2023] accessible via https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay.

ISSN 2281-5147

Is Facebook's reformed commercial practice of 'pay-or-consent' in line with European data protection law in particular and European law in general? The European Court of Justice in its 2023 *Meta* judgment highlighted that 'freely given consent' would imply that consumers are offered, if necessary for an *appropriate* fee, an equivalent alternative where the personal data is not being processed.[5] Are 9,99€ per month an *appropriate* fee and a fair alternative to consenting to the exploitation of our personal data? Thus far, no conclusive answer has been given. For Meta, its Pay-or-Consent model is compliant with the judgment by the European Court. For the European Data Protection Board, offering only a binary choice between either consenting or paying a fee will in most cases not be compliant with European data protection law as it would transform a fundamental right into a feature consumers have to pay for.[6] For the European Commission, Meta's 'Pay or Consent' model would breach the new 2023 Digital Markets Act as it would not offer a true choice to consumers – a truly equivalent alternative should allow consumers to choose an alternative version of the service which is free of (monetary) charge *and* relies on non-personalisation of advertisement.[7]

Which interpretation of the law is correct? If Facebook does not comply with the demands by the European Commission to adapt its commercial practices, the answer will yet have to be given either by the European Court of Justice or through new legislation that clarifies more precisely how we find the equilibrium between the protection of our personal information through the fundamental right to data protection and its economic exploitation by companies.

---

[5] See CJEU case C252/21 Meta v Bundeskartellamt, [2023] ECLI:EU:C:2023:537, para 150.

[6] See Opinion 08/2024 by the EDPB which in reaction to the judgment by the Court argued that offering only a paid alternative to services which process personal data for behavioural advertising should not become the new default way for companies. Whereas the EDPB does not oppose in principle the imposition of a fee to access an 'equivalent alternative', such a fee should not inhibit data subjects from making a 'genuine choice' – whether or not such a fee would be 'fair' in light of the GDPR should fall within enforcement duties of national data protection authorities.

[7] With the Digital Markets Act (DMA) the EU further regulates large digital platforms ('gatekeepers'). Article 5(2) of the DMA requires gatekeepers to obtain consent from consumers if they intend to use their data, for instance, for online advertising services. At the same time, gatekeepers must offer consumers a 'less personalised but equivalent alternative'. For the Commission, Meta's paid subscription model does therefore not constitute an 'equivalent alternative' to the 'free' model that uses personal data for targeted advertisement. See European Commission. (2024). Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act. See also Euractiv. (2024]. European Commission accuses Meta of violating digital competition rules with 'pay or OK' model. Retrieved from https://www.euractiv.com/section/data-privacy/news/european-commission-accuses-meta-of-violating-digital-competition-rules-with-pay-or-ok-model/

ISSN 2281-5147

6. Selected Readings

De Hert, P., & Gutwirth, S. (2009). Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & S. Nouwt (Eds.), *Reinventing Data Protection?* (pp. 3–44). Springer.

De Hert, P., & Lazcoz, G. (2022). When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance. *European Data Protection Law Review*, *8*(1), 31–40. https://doi.org/10.21552/edpl/2022/1/7

EDPS. (2017). *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*.

Euractiv. (2024, July 1). *European Commission accuses Meta of violating digital competition rules with 'pay or OK' model*. Www.Euractiv.Com. https://www.euractiv.com/section/data-privacy/news/european-commission-accuses-meta-of-violating-digital-competition-rules-with-pay-or-ok-model/

European Commission. (2024). *Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act*.

González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer.

Lessig, L. (1999). The Architecture of Privacy: Remaking Privacy in Cyberspace. *Vanderbilt Journal of Entertainment & Technology Law*, *1*(1), 56–65.

Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford University Press.

Mayer-Schönberger, V. (2010). Beyond Privacy, beyond Rights—Toward a 'Systems' Theory of Information Governance. *California Law Review*, *98*(6).

ISSN 2281-5147