UNIVERSITÀ DEGLI STUDI DI MILANO

FACOLTÀ DI SCIENZE POLITICHE, ECONOMICHE E SOCIALI

Data Science for Economics

Cybersecurity and Privacy Preservation Techniques
and
Digital Security and Privacy

The Valorization and Monetization Personal Data:
GDPR Compliances, Business Models of Digital Content and Services and Personal Data Commodification

Hiyab S. Negga
26/11/2023
(Word Count: 4880)

Abstract

This paper examines the data-driven economy, with a focus on digital content and service providers and the various business models currently dominating in terms of data monetization and data valorization. With an emphasis on the European Union and the legal framework of General Data Protection Regulation (GDPR), an inspection of its implementation with a focus on the rights it provides data subjects against extensive profiling for the purpose of monetization is conducted. In addition, a review on the roles of data controllers is undertaken to ensure data subjects' rights. The examination involves assessing different business models by categorizing them as high-risk (such as data as a payment) and low-risk (pay-for-privacy , personal data economy, and privacy-focused model) based on the standards they undertake to process personal data. Relating this with GDPR's protective measures and an attempt to shed light on the challenges faced by high-risk business models, we get to see the endeavor undertaken by big technology companies that are primarily reliant on processing personal data. Despite the efforts unintended consequences, such as market concentration are witnessed. The paper recognizes, debate surrounding the clash between fundamental right and data-as-a-payment is an ongoing one and the need for a case by case evaluation will be at the forefront in settling such intricacies. Overall it is imperative for data subjects to make informed decisions about the digital content or services they use. It is recommended that a shift toward privacy focused service providers would be the best option to obtain the optimal outcome of minimal risk.

Introduction

There is an undeniable surge in the amount of data being generated every month, every week, every hour, of every second.[1] In the latter part of the 20th-century digital transformation has helped us cross from the physical realm into the digital space impacting our lives in all aspects. Most people in developing countries are equipped with sophisticated technology systems running on complex software than previous generations. This has made us a generation that shares every milestone, and personal experience online, increasing our dependence on data-based products or services, and creating a digital footprint that signifies our inherent digital presence as an extension of our lives in the digital ecosystem.[2]

On the other hand businesses and public organizations also rely on the users' data; businesses use the data as a source of insight to strive to get to know their customers, drive down costs improve efficiency and thus indirectly increase their profits, whereas public organizations will require personal data as way to enforce contractual agreements, ensure public safety and other public services that boost the overall wellbeing of the society.

In a digital economy, where data-driven products heavily rely on users' and customers' data has been used in a way that makes it difficult to gauge the actual economic value. In 2017, the European Commission valued personal data[3] to grow to approximately €1 trillion annually by 2020.[4] Similarly, McKinsey estimates that non-generative AI and analytics to be valued at $11.0 trillion to $17.7 trillion.[5] The evolution of digital technologies allows data controllers[6] to access the data generated by users to develop new products and services, resell data to advertisers, provide tailor-made advertisements, and boost their growth.

Data monetization is the process of exploiting personal data for their direct or indirect economic benefits.[7] In this aspect, it is critical to have a clear delineation between data valorization and monetization. Data valorization is the "process of leveraging data to create value within an organization, without necessarily converting it into direct profit" through business activity optimization, cost reduction, and new product rollouts and services.[8] This is also referred to as indirect data monetization, by organizations leveraging insight to transform them into products, services, and new revenue avenues. In contrast, data monetization involves direct selling in raw or insight format to third parties typically practiced in the digital content and service for personalized targeting of users.[9] With the proliferation of digital technologies such as big data analytics, IoT, Cloud, Machine Learning, and AI, data

---

[1] Fabio Durante "Amount of Data Created Daily (2023)", April 3, 2023, (online), accessed November 23, 2023.
[2] Ben Dattner and Tomas Chamorro-Premusiz, How to Curate Your Digital Persona (hbr.org), July 09, 2020, (online), accessed November 23, 2023.
[3] According to the article 4(1) of GDPR, ‹‹personal data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as name, an identification number, location number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.››
[4] European Commission, Fact Sheet - Question and Answers — Data protection reform package, 2017 accessed 19 November 2023.
[5] Mckinsey & Company, Report - The economic potential of generative AI - The next productivity frontier, June 2023.
[6] According to article 4(7), GDPR ‹‹' controller' means the natural or legal person, public authority agency, or other body which alone or jointly with others, determines the purposes and means of such processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller specific for its nomination may be provided for by Union or Member State law;››
[7] Digital technologies: tensions in privacy and data, cit 1301
[8] Boccaccini. P, and Torresan, Camilla, "Data valorization e data monetization, il dato quale asst strategico per il business le sfide", (online) "*Il concetto di data valorization si riferisce al processo che consiste nello sfruttare i dati per creare valore all'interno di un'organizzazione, senza necessariamente convertirli in profitto diretto*". accessed November 24, 2023.
[9] Gartner, Definition of Data Monetization - IT Glossary | Gartner, (online) accessed November 24, 2023. Also see, Boccaccini. P, and Torresan, Camilla, "Data valorization e data monetization, il dato quale asst strategico per il business le sfide", (online), accessed November 24, 2023.

monetization has become a formal discipline, and models beyond traditional business intelligence[10] have been developed.[11]

In the 2018 U.S. elections, scandals such as Meta (formerly Facebook) and Cambridge Analytica served as the stamp of confirmation of misuse of personal data. It entailed 87 million users' data being used without consent to monetize and leverage political gains.[12] Facebook agreed to a payout of $725 million in 2022 to its 250 to 280 million active U.S. resident users from the 24th of May 2007 until the 22nd of December 2022. Similarly, Google became one of the first technology companies to be fined €50 million by the French data protection authority for lack of transparency, inadequate consent permission and inaccessibility, and unclear data processing[13] for personalized advertisements.[14] On the other hand, this does not only pertain to technological companies. A prime example is the Swedish company H&M, which was fined in 2020, for secretly monitoring employees to make a detailed profile influencing decisions concerning their employment.[15] This is indicative that great strides have been made to address the privacy issue to empower data subjects and ensure the consent mechanism transparency and other measures that limit the abuse of personal data by companies whether it is to monetize or valorize.

Even though progress has been made over the past decade, it is important to note that there are major challenges that are still faced to mitigate the risks that make consumers collateral. In the first section of this paper, we will assess the implementation of the General Data Protection Regulation (GDPR) and the key provisions encompassing data subjects and data controllers. Then we will explore the current business model structures of digital content or service providers'[16] and overview the consequences of GDPR on businesses that rely on data monetization through personalized marketing. Lastly, the recurring contention between fundamental rights and the commodification of personal data will be briefly introduced.

GDPR Implementation and Enforcement

Since its implementation on May 25, 2018, the GDPR has been revered as the most robust personal data regulation compared to the rest of the world. Deterrence mechanisms of personal data being processed for marketing purposes such as transparency, fairness, lawful processing, consent[17], access by data subjects of their personal data, data erasure, commonly referred to as the right to be forgotten, data minimization, right to object and so many more gives a moat of security to data subjects to not be subjugated by data controllers or processors to extensive profiling other than the purpose of direct marketing.[18] In this regard, the articles that most stand out that enable data subjects that

---

[10] According to IBM "business intelligence (BI) is a software that ingests business data and presents user-friendly views such as reports, dashboard, charts and graphs to enable business users to access different types of data ,— historical and current, third-party and in-house, as well as semi-structured and unstructured data like social media." — What is Business Intelligence? | IBM accessed November 19 2023.
[11] Joan Ofule and Morad Benyoucef, Data monetization: insight from a technology enabled and research agenda.
[12] ENISA, The Value of Personal Online Data — ENISA (europa.eu), (online) accessed November 19, 2023.
[13] According to article 4(1), GDPR ‹‹'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means such as collecting, recording organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise marking available, alignment or combination, restriction, erasure or destruction';››
[14] Euro News, France fines Google €50 million for "lack of transparency & valid consent regarding advert personalization" using GDPR rules - Business & Human Rights Resource Centre (business-humanrights.org) (online) accessed November 19, 2023.
[15] BBC, Three years of GDPR: the biggest fines so far - BBC News, (online) accessed November 19, 2023.
[16] According to Article 2(1) and Article 2(2) of the Digital Content Directive ‹‹'digital content' means data which are produced and supplied in digital form; 'digital service' means a) a service that allows the consumer to create, process, store or access data in digital form; or b) a service that allows sharing of or any other interaction with data in digital form uploaded or created by the consumer of other users of that service;››
[17] According to Art 4(11) of GDPR ‹‹'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wished by which he or she, by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her;››
[18] EU, "Data Protection and Online Privacy",(online), accessed November 19, 2023.

are citizens or residing in the EU to take a preventative approach to profiling by controllers and processors other than a legitimate interest[19]:

- Article 5: Principles relating to the processing of personal data
- Article 6: Lawful of processing
- Article 7: Condition for consent
- Article 9: Processing of special categories of personal data
- Article 11: Processing which does not require identification
- Article 12: Transparent information, communication, and modalities for the exercise of the right of the data subject
- Article 13: Information to be provided where personal data are collected from the data subject
- Article 14: Information to be provided where personal data have not been obtained from the subject
- Article 15: The right of access by the data subject
- Article 21: Right to object
- Article 22: Automated individual decision-making, including profiling
- Article 32: Security of processing

GDPR deems the protection of personal data in relation to its processing a fundamental right[20], giving more control to natural persons over their personal data.[21] Before any personal data processing is undertaken the data controller must have clear consent that is present to the data subjects in a transparent manner by disclosing the reason for collection, the use of the data, details of other third-party[22] processors, the length of time the data will be kept, in addition to the data protection rights. These protection rights include the right to access, correct, delete, complain, and withdraw consent. With regards to targeted marketing and the issue of privacy the regulation that the data subject should be informed of the existence of profiling and the consequences of such profiling[23].

Data controllers and data processors must comply with stringent requirements when undertaking processing that has the potential to result in a high risk to the data subject. However, processing personal data for direct marketing purposes may be carried out for legitimate interest[24].[25] This can include profiling to display personalized advertisements or sending personalized emails/newsletters without having a significant impact on the data subject with all the pre-requirements taking place prior to collection and processing. “However, with the expectation of marketing emails being sent out on an opt-out basis if the recipient details were collected in the context of the sale of a product or service”.[26] In addition to the articles stated above, data controllers and data processors would keep their data subjects safe from extensive profiling and avoid legal implications if they adhere to:

[19] Legitimate interest may include direct marketing which means if you are an existing customer of a particular customer or a particular company, they can send you direct marketing emails about their own similar products and services with the right to objects at any time.
[20] Personal data is protected as fundamental rights under the European level through the Charter of Fundamental Rights of the European Union (ECHR) 8(1) and the Treaty on the Functioning of the European Union (TEFU) 16(1) clearly stating: “Everyone has the right to the protection of personal data concerning them”.
[21] EU, Regulation (EU) 2016/679, “GDPR” Official Journal of the European Union, April 27, 2016.
[22] According to GRPR Art. 4(10) ‹‹’third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor are authorized to process personal data;››’.
[23] Ibid.
[24] Legitimate interest must comply with the purpose test (is there a legitimate reason behind the processing), necessity test (is the processing necessary for that purpose) and the balancing test (is the legitimate interest overridden by the individual’s interest, right or freedoms).
[25] EU, Regulation (EU) 2016/679, “GDPR” Official Journal of the European Union, April 27, 2016.
[26] GDPR Register, “Direct marketing rules and exception under the GDPR”, November 2, 2022, (onlines) accessed November 25, 2023.

- Article 25: Data protection by design and by default
    - Implements measures such as pseudonymization[27], and data minimization into processing to protect the rights of data subjects
    - Discloses the amount of personal data collected, the extent of processing, and the period of storage.
- Article 26: Joint controller
    - With two or more controllers, they shall be joint controllers who must determine responsibilities for compliance and disclose to data subjects.
- Article 29: Processing under the authority of the controller or processor
    - Any processor acting under the authority of the controller is not permitted to process the data except on instructions from the controller
- Article 30: Records of processing
    - Maintaining processing activities, such as the details of controller and processors, the purpose of processing, categories of data subjects, categories of personal data, categories of recipients, and identification of third countries or international organizations conducted by both data controller and processors.
- Article 35: Data Protection Impact Assessment (DPIA)
    - Controllers must carry out an assessment of impact prior to processing to ensure the protection of personal data.
    - This includes "a systematic and extensive evaluation of personal aspect relating to a natural person which is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;'
- Article 36: Prior consultation.
    - Data controllers must consult with the supervisory authority when a DPIA indicates high risk by providing the purpose and means of processing and measures undertaken to safeguard the rights and freedoms of data subjects.

As of July 2023, six years since GDPR's enforcement over 2000 cases have been recorded of which 711 have reached a final decision.[28] The most common violations are non-compliance with general data processing principles, insufficient fulfillment of data subject rights, the insufficient legal basis for data processing, insufficient cooperation with supervisory authorities, and insufficient technical and organizational measures to ensure security.[29] Although all expose data subjects to external profiling it should be noted the transgression of the top three aforementioned violations introduces direct vulnerabilities to data subjects' profiling for direct economic benefit. Total fines[30] non-compliance with general data processing principles have reached over €1.6 billion, followed by the insufficient legal basis for data processing and insufficient fulfillment of data subjects' rights with over €431 million and over €237 million respectively.[31]

[27] According to GDPR Art. 4(5), ‹‹' pseudonymization', means the processing personal data in such a manner that the personal data can no longer be attributed to a specific data subjects without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measure to ensure that the personal data are not attributed to an identified or identifiable natural persons››';.

[28] EU Press Release, "Data protection: Commission adopts new rules to ensure stringer enforcement to the GDPR in cross-border cases, 4 July 2023, (online), accessed November 22, 2023.

[29] ShardSecure, "What are the Most Common GDPR Violations? A Guide", August 17 2023, (online), accessed November 22, 2023.

[30] According to Article 83(6) ‹‹"Non-compliance with an order by the supervisory authority as referred to in article 58(2), shall in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20,000,000 EUR or in the case of an undertaking, up tp 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher'››

[31] Statistia, "Fines issued for General Data Protection Regulation (GDPR) violations as of May 2023, by type of violation", (onlines) accessed November 22, 2023.

Business Models and Personal Data: Monetization and Valorization

This section gives an overview of the business models mostly used by digital content or service providers to generate profit through marketing by primarily using personal data and those that are privacy-centric to protect users. Delving deeper into the value data controllers generate over personal data by analyzing figures and common practices to give an intuitive level of understanding of the gravity of privacy concerns. In addition, emerging business models that do not track users are mentioned to compare and contrast the practices of data controllers and data processors[32].

There are four overall structures used by companies offering services and products to interact with users' data. The most common two types of business models widely used are data as a payment commonly referred to as the 'zero price model' and paying for privacy which commodifies privacy as a product that can be purchased.[33] This is the classic case in which the data controller asks for personal data from the data subject in exchange for money or valuable service.[34] Big technology companies such as Meta, Google, and X (formerly Twitter) base their revenues on personalized advertisements in exchange for data subjects providing their data to get a service. For example, Meta collects users' information to profile its users based on characteristics such as demographics, interests, social connections, and behaviors to deliver personalized content and recommendations. According to Statista, in 2022 Meta generated $114 billion through its Family of Apps (FoA) segment which includes Facebook, Instagram, Messenger, and WhatsApp of which $113.6 billion of the revenue was generated through social media marketing and advertising[35].

A common practice by service providers is a subscription model that benefits users with an ad-free experience for a monthly payment, commonly referred to as 'pay-for-privacy'. This enables data controllers an alternative scheme to monetize without targeted advertisement. Recent trends have shown that major service providers companies such as Meta, and X are offering a subscription model giving data subjects the choice to continue the platform for free and have their data collected - or pay and completely opt out of targeted ads by removing them.[36] A statement by Meta, clearly specifies they have made changes to the EU, European Economic Area (EEA), and Switzerland based on the GDPR legal precondition of consent to 'address several evolving and emerging regulatory requirements in the regulatory requirement in the region'.[37] In the guidelines of GDPR, the extent of the wording of consent is clearly explained 'if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid'.[38]

The third business model is the personal data economy model with the primary goal of allowing data subjects to gain control, aggregate to derive insights about the data they generate, and even in some cases monetize their data through a data-transfer model under the assumption that data subjects have transferable right or ownership of their personal data (Article 20 of the GDPR states the right the portability).[39] Personal data economy is further dichotomized into data-insight models and data-transfer models. In data-insight models enable data subjects to

---

[32] According to article 4(8) of GDPR ‹‹' processor', means a natural or legal person, public authority agency, or other body which processes personal data on behalf of the controller;'››

[33] S. Elvy, Paying for Privacy and the Personal Data Economy, Columbia Law Review, Vol 117, No. 6

[34] Custer, B. and Malgier, G.(2022) Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data, Computer Law & Security Review Vol. 45, pp. 105683

[35]Statista, "Facebook average user per (ARPU) as of third quarter 2023, by region", (online) accessed November 21, 2023.

[36] Gerken, T., Facebook and Instagram launch ad-free subscription tier in EU (Facebook and Instagram launch ad-free subscription tier in EU - BBC News) accessed November 21, 2023

[37] Meta, Facebook and Instagram to Offer Subscription for No Ads in Europe, "Facebook and Instagram to Offer Subscription for No Ads in Europe | Meta (fb.com)", accessed November 21, 2023

[38] Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on May 2020, pp. 7

[39] S. Elby, Paying for Privacy and the Personal Data Economy, Columbia Law Review, Vol. 177, No. 6 pp. 1393.

become data controllers and remove the concept of data brokers[40] from the supply chain, bringing the data controller (in this case who is the data subject) and the data processor closer.

A UK-based company called Digi.me allows "data subjects to combine data from multiple sources and allows companies to benefit by offering an exchange for personalized service and offers that could include customized discounts."[41] In the case of Digi.me, it ensures its users that its distributed architecture ensures that they never come into contact with or see user information or persuade users how or where they should use their data.[42] When it comes to monetization of data, Digi.me has partnered with a U.S.-based application called Universal Basic Data Income (UBDI) to allow data subjects to 'participate in financial, social, entertainment, and health research studies while protecting their privacy and identity'.[43]

Whereas in data transfer models the concept includes companies serving as a marketplace for data subjects more often to earn monetary compensation for transferring personal data to processors and less often with data insights.[44] For instance, Weople, an Italian-based company prides itself as 'the first bank to invest your data and gain value from it while protecting it and activating your privacy rights'.[45] It functions as follows: data subjects create an account, to which a digital copy of their data from the current controller will be made available on the applicating, in turn, giving users more control over their data to earn Wecoins to increase their visibility and attractiveness to firms which then enables companies to target them through advertising or personalized offers to earn money.[46]

An important question that may be raised is how companies that are practicing in the personal data economy generate revenue. In the case of Digi.me, which poises itself as postman charges the receiver of the data $0.10 per share with a maximum cap of $3.00 per year per individual per business.[47] Whereas their strategy partner UBDI disclosed in an interview with the podcast Marketplace Tech, that the company collects 20% of what companies are paying to the data subjects.[48] Weople have a similar structure with a different scheme of compensation where the data subjects expect a transfer of 90% of the value generated. [49]

On the other end of the spectrum are the fourth business model service providers that are privacy-focused but ad-supported or subscription-modeled companies. Companies like DuckDuckGo, BraveBrowser, and ProtonMail are the few to name operating with a privacy-focused or privacy-by-design business model. However, each of them has a different means of monetizing their businesses and it is important to emphasize that they do not rely on personal data collection to monetize.

DuckduckGo offers a search engine alternative to Google, which does not track you when you visit their search engine or other websites (third-party trackers).[50] The company offers its users free protection with its private search engine making you unidentifiable, blocking trackers, and application tracking protection.[51] Its approach is to collect

---

[40] Data brokers is a business that aggregates information from a variety of sources; processes it to enrich, cleans or analyze it; and licenses it to other organizations.
[41] Ibid, 1395 -1396
[42] S. Elvy, Paying for Privacy and the Personal Data Economy, Columbia Law Review, Vol 117, No. 6
; MEF Whitepaper, Understanding The Personal Data Economy: The Emerging of a New Data Value Exchange, pp. 11; Digi.me, 'About', https://worlddataexchange.com/about, accessed November 21, 2023.
[43] Wheeler, P., "UBDI's data monetisation platform launches in Europe-Digi.me", accessed November 21, 2023.
[44] S. Elvy, Paying for Privacy and the Personal Data Economy, Columbia Law Review, Vol 117, No. 6
[45] Weople, https://weople.space/en/, accessed November 21, 2023.
[46] Ibid.
[47] Government of UK, Digi Me Response (publishing.service.gov.uk), accessed November 21, 2023.
[48] Budzyn, D, Wood, M., An app that pays your for your data, https://www.marketplace.org/shows/marketplace-tech/an-app-that-pays-you-for-your-data-yes-actually/, accessed November 21, 2023.
[49] Weople, Functions, https://weople.space/en/#functions, accessed November 21, 2023.
[50] DuckDuckGo, DuckDuckGo Privacy Policy, accessed November 22, 2023.
[51] DuckDuckGo, Inc, "DuckDuckGo's comments regarding the ACCC's upcoming report on market dynamics and consumer choice screens in search services and web browser"[online], April 12, 2021.

minimal data (data minimization[52]) such as IP address, browser type, and language only provide the information users have requested, and ensure that it's not a malicious bot that is making the request.[53] Despite using them to deliver content the data is not stored or logged for further use the company vows only search queries are being saved completely disconnected from personally identifiable data.[54] The company monetizes "based on contextual search advertising, which is based on the context of the page you are viewing, as opposed to behavioral advertising, which is based on the detailed profile (profiling[55]) about you as a person". [56]

BraveBrowser takes the privacy-focused policy one step further by not tracking users or queries and allowing users to either block advertisements altogether or they can use their browsing application to monetize the private advertisements they actually view through their Basic Attention Token (BAT) to earn 70% of the revenue share on the basis that users opt-in.[57] The company stands out from its competition because of its aggressive approach to blocking advertisements that lure users to click on them are disabled even on other browsers, it blocks cookies, and phishing attempts.[58]

Lastly, ProtonMail uses a subscription model and adheres to the privacy laws where it is based, Switzerland. Founded in 2014, by scientists at CERN, ensures data subjects offer free service of end-to-end encryption and privacy with no third-party transfers.[59] Users can upgrade with a subscription with more features but a basic (free) option is also available as the company believes privacy to be a human right.[60]

The privacy-focused user base has been growing yearly with BraveBrowser's monthly active users starting out at 1.2 million in 2017 to 50.2 million in 2022. In addition, 8 million users monetize privacy-preserving Brave Ads and the search engineer receives 2.3 billion queries annually.[61] According to Cloudflare DuckDuckGo has also managed to obtain the second largest market share for mobile search in Europe and the U.S.[62] ProtonMail has also surpassed 70 million user accounts as of 2022.[63] This is indicative of data subjects valuing the privacy of their personal data and how it is being used. We consider these companies to uphold data valorization techniques as they do not collect personal data that is identifiable to the user to gain direct profit, they are rather focused on privacy and strive to create a seamless experience for their users.

To develop the idea we will characterize data-as-a-payment as high-risk data-driven business models because they rely on personal data as a revenue stream (monetization).[64] Whereas pay-for-privacy, personal data economy, and privacy-focused are characterized as low-risk-data-driven businesses that rely on the use of data to improve a company's operation or products or services (valorization). In the next section, we will focus on high-risk-data-driven, especially on data as a payment business model and the impact of GDPR and its unintended consequences.

---

[52] According to GDPR, Art 5(1) c, data minimization is the practice of collecting 'adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed'.
[53] Ibid.
[54] Ibid
[55] According to GDPR Art. 4(4), ‹‹'profiling' means any form of automated processing of personal data consisting of the user of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health personal preferences, interests, reliability, behavior, location or movements;·››'.
[56] DuckDuckGo, Inc, "DuckDuckGo's comments regarding the ACCC's upcoming report on market dynamics and consumer choice screens in search services and web browser"[online], April 12, 2021.
[57] Brave, Brave Search privacy notice | Brave Search. See Also Brave, Brave Ads | Brave, accessed November 22, 2023
[58] Azza Mohammed and Ibrahim Ismail, "A Performance Comparative on Most Popular Internet Web Browser', 4th International Conference on Innovation Data Communication Technology and Application, (2023): 548
[59] Proton, Proton — Privacy by default, accessed November 22, 2023.
[60] Ibid.
[61] Brave, Brave Passes 50 Million Monthly Active Users, Growing 2x for the Fifth Year in a Row | Brave, accessed November 21, 2022.
[62] Cloudflare Radar, Cloudflare Radar, accessed November 22, 2023.
[63] Proton, Proton reaches 70 million accounts | Proton, accessed November 22, 2023.
[64] Josua New and Christina Montgomery, "Precision Regulation for Data-Driven Business Models".

Impact of GDPR reduction of monetization and increase of 'valorization' and its unintended consequences

As we have examined the legal aspect of the GDPR with respect to processing personal data for economic benefit, it is also worth presenting how these have affected real users and the business models stated in the previous section that heavily rely on third-party marketing data. It is evident that companies that collect and process data for profiling and marketing operating with the data-as-payment business model will have more difficulty continuing their monetization strategies. It will force marketers to relinquish their dependence on behavioral data collection which will implicate businesses that primarily depend on digital ad targeting without consent.[65]

Even though this came as a challenge to the larger tech companies such as Facebook and Google, evidence shows that they have managed to strengthen through internal data transfers for target advertising by gaining user's consent.[66] Following the GDPR, Google first put restrictions on advertisers seeking perspective on data generated from ad buys in its ecosystem and removed encrypted cookie IDs, IP addresses, and user list names from data transfer for all bids in Google AdExchange.[67]

Data-sharing limitations and the shift from third-party to first-party cookies have increased market concentration by 17% putting small vendors[68] at a disadvantage.[69] Through the administration lens, small, medium-sized, and large companies have seen high compliance costs.[70] The EU surveyed 716 small business leaders in Europe about GDPR compliance with around half failing to comply with respect to disclosing processing activities to data subjects and identifying a lawful basis.[71] The drop in market share of small vendors is attributed to a lack of compliance resources that compels website owners to opt for safer ad choices as a result.[72] This shows that as a way to remain compliant with GDPR requirements large technology companies have made attempts to shift from the processes of monetization to "valorization".

As a result, big tech has been inundated by allegations and fines through antitrust cases in European countries. In 2021, the Italian antitrust regulator fined Google and Apple €10 million each because they had not provided 'clear and immediate information on how they collect and use data of those who access their service' as well as an 'aggressive' approach to nudge[73] users to 'accept the commercial processing'.[74] In a more recent article by Reuters, Google confirmed changing its user data practices to terminate an investigation by German antitrust which is 'aimed

---

[65] Dipayan Ghosh, "How GDPR Will Transform Digital Marketing", May 21, 2018, (online), accessed November 23, 2023.
[66] Aryamala Prasad, 'Unintended Consequences of GDPR', (online), accessed November 23, 2023.
[67] Alison Weissbrot, "Google Sharply Limits DoubleClick ID Use, Citing GDPR", (online) accessed, November 23, 2023.
[68] In the study by Johnson, G and Shriver, S, vendors are defined as web technologies that support services to the website including: raising ad revenue, hosting audiovisual content, measuring visitor activity, and facilitating social media sharing by processing large-scale personal data processing. The leading companies are Google and Facebook which capture 56% of global digital advertising spend.
[69] Dipayan Ghosh, "How GDPR Will Transform Digital Marketing", May 21, 2018, (online), accessed November 23, 2023. See also Garret A. Johnson & Scott K. Shriver, "Privacy & market concentration: Intended & Unintended consequences of the GDPR", January 20, 2020.
[70] Aryamala Prasad, 'Unintended Consequences of GDPR', (online), accessed November 23, 2023.
[71] EU, "Millions of small businesses aren't GDPR compliant, our survey finds", (online), accessed November 23, 2023.
[72] Whotracks.me, "GDPR - What happened"?, September 3, 2018, (online), accessed November 24, 2023.
[73] Shara Monteleone, et.al, "Nudges to Privacy Behavior: Exploring an Alternative Approach to Privacy Notices", defines nudges, as ‹‹"changes in the choice architecture to elicit a certain behavior, have been shown to be effective in other domains'.››
[74] Reuters, "Italy court rejects Google's appeal against watchdog fine accepts Apple's one', November 18, 2022 (online) accessed November 24, 2023. See also, Natasha Lomas, "Italy fines Apple and Google for 'aggressive' data practices", November 26, 2021. (online) accessed November 24, 2024.

at curbing its data-driven market power' this is expected to 'give users more choices on how their data is used'.[75] These probes are not limited to Google; it includes Amazon, Meta, and Apple.

Business models that abide by a pay-for-privacy business model may result in the exclusion of the economically vulnerable part of society due to privacy being considered a luxury that is available only to those who can afford it.[76] In contrast, the personal data economy provides a marketplace for users to transfer their data (or rights in the data) directly to the PDE company or unaffiliated third parties for the monetization of data subjects and the company.[77] The example of Weople invokes Article 20 of the GDPR which ensures the data subject's right to data portability and transmit it but not without the challenge of abuse from dominant companies.[78] However, the data-privacy-business model mentioned in the earlier section stays clear of any personal data processing beyond legitimate interest.

It is evident at the center of GDPR data subjects' personal data protection to excessive profiling, right to privacy, and their freedoms by minimizing or eliminating any risk that may expose them to misuse or abuse of their data. Since its implementation there has been a growing awareness of data subjects, however between commercial interests seeking maximum monetization of consumer information and consumer's control over their personal data, consumers are nudged to provide personal data freely.[79] A field experiment conducted by MIT has shown two critical characteristics that could be used as an explanation as to why data subjects are susceptible to data-as-payment. People who have high regard for their privacy are willing to waive private data quite easily when incentivized to do so, and whenever privacy requires additional effort or comes with a smoother user experience, participants are quick to abandon technology that would offer them greater protection.[80]

With data-as-payment and pay-for-privacy business models being the simple component of the price users pay for the purchase of the primary service, the value of their personal data may exceed the value of the products or services they receive for free or the price presented.[81] Thus a recent trend that highlights the asymmetry between data subjects and data controllers with regard to the value of personal data and uses of personal data could be deterred by informing the quantitative value of personal data calculated on objective parameters.[82]

GDPR and Fundamental Rights: Commodification of Personal Data

The awareness of the economic value of personal data by data subjects, especially in the marketing industry has grown significantly since the implementation of the GDPR and consequently, the issue of personal data commodification has become a point of contention. GDPR specifies the protection of personal data as a fundamental right, giving control to data subjects over their personal data but does not consider it as a tradeable commodity.[83] As

[75] Friederike Heine, Reuters, "Google changes user data practiced to end German antitrust probe", October 5, 2023, (online), accessed November 24, 2023.
[76] Milena Murisa and Carmine Andrea Trovato, "The commodification of our digital identity: limits on monetizing personal data in the European context"
[77] S. Elvy, Paying for Privacy and the Personal Data Economy, Columbia Law Review, Vol 117, No. 6
[78] Weople, "The Italian Competition Authority publishes the commitments files by Google, aimed at overcoming the investigation for abuse of dominant position, in particular against Weopel", March 2023, (onlines) accessed November 24, 2023.
[79] Milena Murisa and Carmine Andrea Trovato, "The commodification of our digital identity: limits on monetizing personal data in the European context"
[80] Athey, S., Catalini, Tucker, C., "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk", National Bureau of Economic Research, June 2017.
[81] Ibid.
[82] Milena Murisa and Carmine Andrea Trovato, "The commodification of our digital identity: limits on monetizing personal data in the European context",
[83] Marco Propato and Luca Zanoni, "The debate over data monetization - an EU (and Italian) perspective", June 13, 2022, (online) accessed November 25, 2023.

a fundamental right implies that it is an inalienable right and thus people can not waive or transfer the right making the ownership of data and the data economy based on personal data as a commodity difficult to reconcile.[84]

The business model described above, especially data as a payment model, considers personal data as currency but under EU law it cannot be reduced to a mere economic asset.[85] The Chairman of the Italian data protection authority (Garante) has gone as far as condoning the deed of monetization of consent as "monetization of freedom and the ref-eudalization of social relationships to the detriment of the most vulnerable persons".[86] This is also clearly stipulated in the Digital Content Directive (DCD), Recital 24, which states that digital content or digital services are often supplied where the consumer does not pay a price but provides personal data and with the recognition of personal data as a fundamental right personal data cannot be considered as a commodity.[87]

On certain occasions, the right to data protection as a fundamental right might not justify a restriction to freedom of contract of individuals has been raised as a way to counter the claim that data should not be a tradable commodity.[88] In 2020, the court of Lazio accepted that personal data could constitute a commercial asset for the counter-performance of a contract in a technical sense if operators comply with necessary requirements.[89] The Supreme Court of Italy affirmed as long as the exchange is based on consent that is not coerced data subject access to a service to consent to unnecessary data processing as long it is not essential, not unique and the possibility of offer remuneration is also open.[90] This is also applicable in the practice of French and Austrian Data Protection authorities, which consider the 'pay or consent' valid, and some view this as a recognition of the monetary value associated with the use of data.

Conclusion

So far we have seen the importance of the data-driven economy with service providers utilizing personal data to monetize and valorize their business. We explored business models, namely, data-as-a-payment is characterized as high-risk business models because they pose some threat to the processing of personal data beyond legitimate interest. Nevertheless, low-risk-data-driven models such as pay-for-privacy, personal data economy (data-insight and data transfer models), and privacy-focused businesses minimize the risk of unnecessary processing of personal data and ensure the data subjects consent providing awareness and more control.

In addition, we explored how the GDPR protects data subjects from being subjugated to extensive profiling beyond their legitimate interest and stated the principles that keep them from being subject to such practices. Similarly, as per the GDPR we inspected the roles data controllers could serve in the interest of data subjects and deter their organization from non-compliant fines. High-risk modeled businesses, especially those that undertake data-as-a-payment face difficulty in complying with the GDPR are more susceptible to non-compliance penalties. Even though major changes are undertaken and are going at great length to adapt to the new paradigm shift of a user-centric with right privacy right being at the center of the issue under the GDPR, there are unintended consequences that resulted in market concentration.

---

[84] Bart Custers and Gianclaudio Malgeri, "Priceless data: why the EU fundamental right to protection is at odds with trade in personal data", 2022.
[85] Milena Murisa and Carmine Andrea Trovato, "The commodification of our digital identity: limits on monetizing personal data in the European context"
[86] Marco Propato and Luca Zanoni, "The debate over data monetization - an EU (and Italian) perspective", June 13, 2022, (online) accessed November 25, 2023.
[87] EU 2019/770 "on certain aspects concerning contracts for the supply of digital content and digital services", May 20, 2019.
[88] N. Purtova "EU Data Protection Law - Current State and Future Perspective",
[89] Michele Dierens and Wannes Ooms, "Personal data as a commodity: is the door open for small-scale data processing?", 04 August, 2022, (online) accessed November 25, 2023.
[90] Milena Murisa and Carmine Andrea Trovato, "The commodification of our digital identity: limits on monetizing personal data in the European context"

Finally, we saw the point of contention between the fundamental right and the GDPR and the use of the data-as-a-payment model remains an open debate and left to be evaluated on a case by case basis. Recognizing the dangers associated with processing personal data through extensive profiling and the importance of privacy, it is recommended to data subjects to make conscious decisions about the service providers they choose. Shifting to privacy-focused service providers would enable them to minimize the risk that may otherwise be imposed by other business models.