Data Monetization and User Consent: Better Privacy or More Bureaucracy?

Authors: Rolf Auf der Maur & Delia Fehr-Bosshard

>> Entertainment Business Opportunities

As consumers are less willing to pay for content, the media and entertainment industry is constantly looking for new channels to generate revenues. Increasingly, value is created through the collection and processing of user data. Monetization of data can be done externally or internally. External monetization means selling data to interested third parties. The internal use of data by applying data analytics methods for the media and entertainment business is much more creative: it allows for new and better products in the digital sphere through personalization of content and targeting of advertising. The business opportunities in the wake of big data analytics for media and entertainment are still at an early stage but appear to be almost unlimited. The following use cases are therefore far from being exhaustive and only intended to facilitate the discussion of relevant privacy issues affecting the operators of online media and entertainment platforms:

1) Optimization of products and services through data analytics to **understand the preferences of customers and connect with audiences** across channels, e.g. through "recommendation engines" based on customer insight;
2) facilitating **more efficient** provision of services, e.g. streamlining processes, eliminating unnecessary or irrelevant steps, refraining from unsuccessful marketing activities;
3) supporting organizations to **reduce risks,** e.g. by evaluating the financial potential of customers;
4) **development of new products and services** and identifying new markets and market

segments, e.g. with multiple paid content offerings which adapt dynamically to user preferences and willingness to pay;

5) **mitigating risk of information overload** by providing relevant content, instead of just more information;
6) **relevant and efficient advertising** through profiling and targeting;
7) **merger of the product and its marketing,** e.g. through methods known as "growth hacking", where the service itself is used for marketing instead of traditional advertising in order to rapidly increase the user base, as done for instance by Facebook when introducing buttons and widgets and YouTube with its recommendations for videos to share and recommend, creating a viral loop.

Leading online businesses such as Facebook create value almost exclusively by using (personal) data. Facebook does not offer a paid product alternative without collecting data and generating revenues through targeted advertising. Traditional players in the entertainment industry might still be reluctant to give their products away for free but they increasingly apply data analytics to optimize their offers.

>> Data Protection Challenges

Not all data used for high quality analytics need to be "personal data", i.e. information allowing the identification of an individual. In the age of "big data", information from different sources (personal data, sensor data, geographic date, and machine data to name a few) is combined for analytical purposes. The more (initially non personal or anonymized) data are put together, the more such data become attributable to an individual and, hence, personal. If personal data is collected or processed, this generally triggers data privacy laws and regulations. With big data analytics, it has become more difficult to argue that data are anonymous and out of scope of privacy regulation. The regulatory framework for the collection and processing of personal data is fragmented: **national, regional and sector-specific laws and regulations** govern the extent of permissible collection, processing and transfer to third parties of personal data with and without consent.

An important recent development for the entertainment business is the new EU General Data Protection Regulation[1] ("GDPR"), becoming effective in May 2018, which significantly widens the **territorial scope** of EU data privacy regulation: the GDPR applies to processing of personal data from any data subject anywhere in the world if the data controller or processor has an establishment in the EU and the data is processed in the context of the activities of such an establishment.[2] The GDPR also covers data collection and processing of a controller or processors outside of the EU, if the respective data subjects are in the EU and the activities are related to either of the following:

- The offering of goods or services to data subjects in the EU, regardless of whether a payment of the data subject is required; or
- the monitoring of behavior of data subjects in the EU as far as their behavior takes place within the EU.[3]

A media company, e.g., offering its subscription services in the EU and processing the customer's data in connection with these activities, falls within the scope of the GDPR, regardless of whether the company itself is located in the EU or not. For companies using personal data, **governance efforts** necessary to maintain the legal handling of data will increase. Besides more detailed information and consent requirements (see next paragraph below), more documentation is needed under the GDPR. It is possible and very likely for internationally operating businesses to fall within several data protection jurisdictions and to be supervised by different data protection authorities in and outside the EU. If the company is not domiciled in the EU, the GDPR does not foresee a lead supervisory authority within the EU, but technically allows for every involved member state to act individually.

In case of violations of the GDPR, and further to potential civil claims for damages,[4] **criminal sanctions** include fines of up to EUR 20'000'000 or 4% of the last worldwide annual turnover (whichever is higher).[5]

Besides legal and regulatory requirements, contractual restrictions, e.g. in commercial contracts, licenses or NDAs, may further limit the use of accumulated data.

Companies are advised to review and potentially revise end-user license agreements (EULAs) and privacy policies when planning new ways to monetize data.

>> Informed User Consent

Even though data privacy is of increasing concern to the public in general, individual users rarely make use of the control mechanisms in place. Users generally do not read the long and complicated privacy policies. Even users who read privacy policies often do not understand how to make use of data control options. Users who disagree with the terms of a privacy document do not usually change the standard wording and send back a redlined version to the provider before using the services. They know that the provider would not be willing to accept any changes. As a result, online services are designed as "take it or leave it" offerings. The current concept of **informed user consent** – by checking a box, clicking on "I read and agree" or just continuing using a website after having been informed of the existence of a privacy policy – remains largely a fiction in the age of big data analytics. The GDPR intends to improve the position of the user by providing more information and ways to control the use of personal data. It requires more transparency and especially the following **information,** amongst others, prior to the collection of data:[6]

- the name and contact details of the controller;
- the purpose of the data processing and the relevant legal basis;
- legitimate interests pursued by the controller or by a third party;
- recipients or categories of recipients of the personal data;
- retention periods;
- rights of the data subject (e.g. erasure of personal data or restriction of processing);
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract; and
- the existence of automated decision-making.

For any processing for a different purpose, the controller needs to provide the data subject with prior information on that other purpose. The information needs to be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[7] As longer privacy policies do not necessarily provide better information, the GDPR at least acknowledges that information may be conveyed through standardized symbols.[8] This hopefully allows for a **more creative and attractive communication** of data privacy issues, as opposed to the current practice of long and complicated privacy policies.

Leveraging data might require the combination of information on the same data subject from different sources. Whereas transparency requirements are usually quite straight forward for direct collection of data from the data subject, the implementation is more complicated if personal data is matched from **different sources.** The controller (i.e. the person receiving and using the data but potentially including the disclosing party as well) is responsible for providing the data subject with additional information on, amongst other things, the source of the personal data and, if applicable, whether the data came from publicly accessible sources or not.[9] This information needs to be provided at the latest within a month after obtaining the personal data, at the time of the first communication to the data subject or the disclosure to other recipients.[10]

The GDPR limits the **formats of acceptable consent.** Only a "clear affirmative act" qualifies as valid consent. In particular, pre-ticked boxes or inactivity of the user are not sufficient as user consent.[11] For providers of online platforms and services, the balance between data privacy compliant consent formats and usability and attractiveness of the services will become more challenging.

Consent needs to be given freely, i.e. the performance of a contract, including the provision of a service, should not be conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[12] Sweepstakes and contests must therefore not require the participant to consent to the use of data for marketing purposes in order to participate and win.

The data subject may withdraw his or her consent at any time,[13] leaving the processing company at risk on whether the data analytics foreseen by the business model may be further pursued in the future.

"For providers of online platforms and services, the balance between data privacy compliant consent formats and usability and attractiveness of the services will become more challenging"

>> Other Justifications for Data Monetization

Valid and documented **consent** is and will remain the most compliant and risk-reducing basis for data use and disclosure. The GDPR, however, acknowledges other justifications for collection and use of data than user consent. This includes processing necessary for the performance of a contract with the data subject,[14] or for legitimate and overriding interests pursued by the controller or a third party.[15]

Data processing might be necessary for the **performance of the contract** with the user and thus justified even without specific consent, e.g. for recommendation engines and other customized services and products (no. 1 above), streamlining processes for services (no. 2), personalization of products and services in general (no. 4), reducing information overload and providing tailored news (no. 5) as well as measures of growth hacking (no. 7). Examples which are unlikely to qualify for this justification include the sale of personal data to a third party (external monetization), targeted advertising (no. 6, without the user preliminary requesting specific offers) and data processing to reduce risks prior to entering into a contract (no. 3) not at the request of the data subject.

The GDPR explicitly references "**direct marketing" as legitimate interest.**[16] It is unclear at this point, how far-reaching this exception for own or third party marketing purposes will be interpreted by the competent authorities. Whether and to what extent targeted advertising measures (no. 6) can be justified by the **business interest of direct marketing** alone, absent any specific user consent, will need to be defined through practice and will be crucial for the advertising business. As advertising revenues help support valuable free content and independent journalism, the media, entertainment and advertising industries will have to raise public awareness for their interests and develop standards and practices which further the acceptance of online advertising practices. The recently established "coalition for better ads" (www.betterads.org) is an important step for the industry, as it encompasses the biggest operators of online platforms, advertising networks and international industry organizations.

>> Risk Focused Approach

More mandatory information and longer privacy policies alone presumably do not lead to more effective control of data by the users. Consent requirements alone are not able to properly mitigate severe risks of big data analytics, such as **discriminatory automated decisions** negatively affecting the rights and interests of individuals, filtering on the basis of non-transparent algorithms or the risk of **data breaches** on big scales.

A more risk-based approach in regulation (as already applied selectively in the US) would allow for prohibiting or limiting **high-risk practices** (e.g. automated decisions in highly sensitive fields like health, social security, financial services and job applications) while allowing rather low-risk data uses (e.g. customization of advertising according to user defined preferences for consumer goods, personalization of a media platform starting page).

On a **legislative** level but also for **self-regulation,** the risk-based approach provides for a more proportionate regime, balancing the rights of the data subject, on one side, and of the data controller and processer, on the other. Data controllers and processors should think about adequate self-regulation for their specific practices to address the respective industry's needs but also provide guidelines for **authorities and courts** on best practice in a particular field. Further, a (legislative) mandate to the competent authorities and courts to follow the risk-based approach when interpreting the law allows them to consider the actual risks (and opportunities) of data processing for both sides – the data subject as well as the data controlling or processing party.

The **GDPR** follows this approach at least partially by addressing potential high-risk practices (e.g. in its provisions on automated decisions, impact assessments and data breach notices). However, it is questionable whether the EU model with its general prohibition of data processing without a specific legal basis (e.g. informed consent, legal obligation, legitimate business interest) adequately addresses the media and entertainment landscape with its many low-risk data processing applications. In the interest of the European media and entertainment industry it is to be hoped that "direct marketing" as a legitimate interest in the sense of the GDPR will be interpreted widely and also cover state of the art tracking and targeting methods that are indispensable for the generation of online advertising revenues. A limiting interpretation of the "direct marketing" interest will result in a shift of advertising spend to platforms operated outside of Europe and to the growing category of native advertising (e.g. paid content, sponsored posts and corporate publishing).

Examples of potentially **low-risk use cases** in the entertainment and media industry include recommendations of products based on user preferences (no. 1 of the above referenced use cases), streamlining processes and marketing (no. 2), creating new products and services to serve customer needs (no. 4), most applications of targeted advertising (no. 6) and using the product or service itself to advertise (no. 7). A higher risk might be associated in the individual case with automated risk determinations and decisions, e.g. based on financial information or detailed profiling of the individual (no. 3). In extreme cases of content personalization in the form of tailored news and information, targeting might exceed what is necessary as a pragmatic response to information overload and instead create a threat for the individual's interest to information (no. 5).

The risk of privacy violations can generally be mitigated by **anonymization** or at least **pseudonymization** of data. The tradeoff is a reduced utility for customization of products and services. The more personal and sensitive data is collected and used, the higher the risk in case of a data breach or misuse.

Creative business solutions might include product differentiation between user preferences: users who would like to use a service freely and including the benefits of personalization are asked to provide explicit consent for specific data to be shared for customization and development of services and the like, depending on such data. Other users not willing to share data will be offered another version of service or subscription – without certain benefits and/or against payment of a fee. The residual risk under the GDPR of consent not freely given and therefore being invalid will have to be clarified through practice. It is up to the individual service provider to render their data-based product as relevant as possible to make it **more attractive for users** to provide their valid consent for data collection and processing.

[1] *Regulation EU 2016/679.*

[2] *Art. 3 para. 1 GDPR.*

[3] *Art. 3 para. 2 GDPR.*

[4] *Art. 82 GDPR.*

[5] *Art. 83 GDPR.*

[6] *Art. 13 GDPR.*

[7] *Art. 12 para. 1 GDPR.*

[8] *Art. 12 para. 7 GDPR.*

[9] *Art. 14 para. 2 letter f GDPR.*

[10] *Art. 14 para. 3 GDPR.*

[11] *Consideration 32 GDPR.*

[12] *Art. 7 para. 4 GDPR.*

[13] *Art. 7 para. 3 GDPR.*

[14] *Art. 6 para. 1 letter b GDPR.*

[15] *Art. 6 para. 1 letter f GDPR.*

[16] *Consideration 47 GDPR.*