

# The value of big data

## GDPR'S IMPACT ON TELECOMS OPERATORS AND BIG INTERNET FIRMS



There is great excitement about big data and machine learning, and the range of uses they can support to offer improvements in our daily lives. However, this excitement is tempered by nervousness about exactly how the data will be used and how much power will be wielded by organisations that gather masses of personal data.

Telecoms operators and large internet players both rely heavily on data, but in quite different ways. In this note, we analyse the differences and then go on to discuss the potential impact of the new General Data Protection Regulation (GDPR)<sup>1</sup> on these companies.

### Exponentially increasing data usage

The volume of data carried over both fixed and mobile networks is growing exponentially; the variety of data spawned is also multiplying as new types of applications, such as 'personal helpers'<sup>2</sup> emerge. This is creating a personal digital trail that reveals a lot about us, from where we tend to be at certain times of the day to what's on our minds. It is well established that how we say we will behave in particular situations differs from the way we behave in practice. The data that is collected via our 'internet usage trail', unlike when we respond to surveys, reflects our *actual* behaviour. A key question is to what extent companies can turn this data into meaningful information that can be monetised.

### Turning data into money

In broad terms, it is possible to use data generated by users to increase profits by:

- Improving the products that are offered by the holders of the data (a one-sided business model);
- Improving the effectiveness of products offered in a different market (a multi-sided business model) e.g.:
  - Using data to increase the effectiveness of ads; and
  - Offering the data commercially to other organisations to allow these organisations to improve their offers to their customers and/or make better decisions, based on better insights into the behaviour of existing or potential customers.

Telecoms operators and large internet players have access to a wide array of data on users that they tend to harness in quite different ways, as discussed below.

---

<sup>1</sup> GDPR came into effect on 25 May 2018.

<sup>2</sup> For example, smart home devices, such as Google Home and Alexa, will mean that new types of data on users are being generated. For example, see <https://techcrunch.com/2017/11/08/voice-enabled-smart-speakers-to-reach-55-of-u-s-households-by-2022-says-report/>

## Telecoms operators

Telecoms operators can have information on areas, such as the demographic characteristics of their customers, what sites they visit, what apps they are running and their usage patterns<sup>3</sup>, and what devices they are using. In addition, mobile operators have extensive data on the movement of their customers, as their phone is constantly communicating with surrounding base stations. They can employ all of this data in a number of different ways<sup>4</sup>:

1. **Optimising network performance.** Fixed and mobile operators use data to monitor network faults and incipient congestion to help them decide where more investment is needed.
2. **Designing tariffs and identifying opportunities to tailor product offers.** For instance, operators know when you are about to exhaust your monthly data allowance or what time of day you tend to use your phone or other device. More insights could be drawn from this type of data by applying findings from behavioural economics. For example, behavioural economics could be used to gain a deeper understanding of why some customers regularly switch providers whereas others' don't.
3. **Selling ads.** To date, most telecoms operators (fixed and mobile) have not focused much on trying to sell ads<sup>5</sup>, although some mobile firms have tried to monetise targeted bulk Short Messaging Service (SMS) advertising and other initiatives<sup>6</sup>.
4. **Aggregating data to provide insights into customer behaviour for other organisations.** For instance, mobile operators' data can provide pointers to where it may be worth locating new stores or what transport services would best serve towns. Telefonica has set up a business unit to provide such insights<sup>7</sup>. In general, even though this type of service does not directly involve offering personal data (since the data is aggregated), telecoms operators have still been wary of potentially breaching privacy protection legislation and undermining customer trust. For example, Deutsche Telekom cancelled a pilot project on the analysis of customer data to improve traffic management in Nuremberg<sup>8</sup> due to privacy concerns<sup>9</sup>.

## Large internet players

If it is technically feasible to collect data on *something*, chances are that large internet players are doing it. Depending on the player in question, data is held on things like location history, photos, documents uploaded, calendars, messages sent, searches made, pages that have been "liked" or shared, music listened to, etc.<sup>10</sup>

<sup>3</sup> In technical terms, operators are able to 'identify' what is in the header of data packets, which allows them to gain some insight into what type of content is being transmitted without seeing the content itself. In the absence of end-to-end encryption e.g. Whatsapp, telegram etc - operators are also 'able' to see the content itself should they choose to.

<sup>4</sup> See for example [https://www.ofcom.org.uk/\\_data/assets/pdf\\_file/0020/92153/online\\_customer\\_data.pdf](https://www.ofcom.org.uk/_data/assets/pdf_file/0020/92153/online_customer_data.pdf)

<sup>5</sup> There appear to be some exceptions. For example, Verizon in the US has acquired both AOL and Yahoo in an attempt to take on Google and Facebook in advertisements. (<https://www.forbes.com/sites/greatspeculations/2017/06/14/where-will-verizons-oath-stand-in-the-digital-advertising-market/#56d5ac89495a>).

<sup>6</sup> In the UK, O2/Vodafone/EE launched a joint venture (Weve) that offered a payments platform with targeted advertisements. However, Vodafone and EE have since left the joint venture.

<sup>7</sup> <https://www.telefonica.com/en/web/press-office/-/telefonica-launches-luca-its-new-big-data-unit-for-corporate-customers>

<sup>8</sup> Deutsche Telekom was planning to provide information on how traffic flowed through the city and how frequently different means of transport were used.

<sup>9</sup> <https://global.handelsblatt.com/companies/telecom-firms-in-big-data-push-626375>

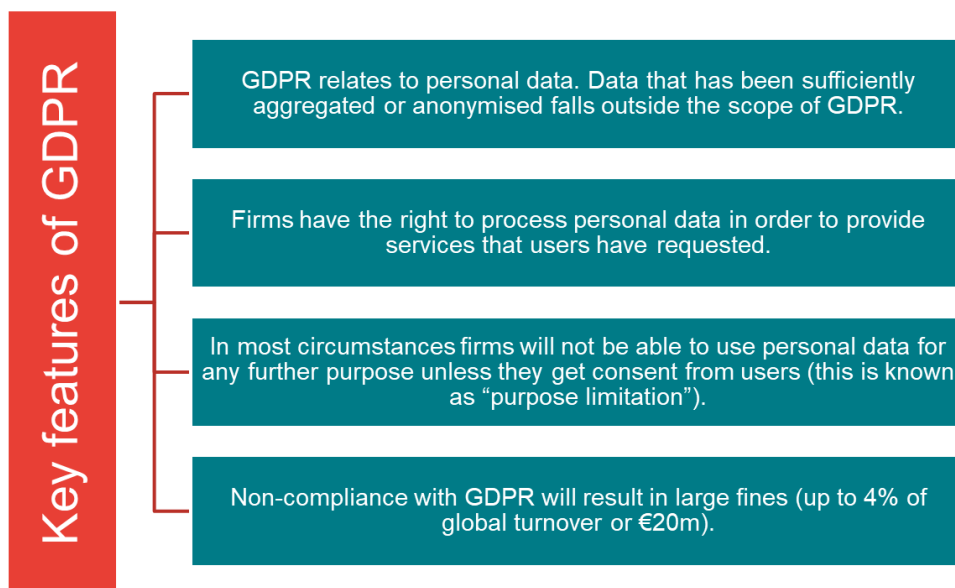
<sup>10</sup> Google and Facebook actually let users/members download the data they have on them. See <https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy>

Of course, collecting data is central to the business of a number of internet players. Many offer their services for free or at a very low cost, with the aim of maximising the number of users of the service. Revenues are then generated from ads that are targeted to the users of the service. Large internet companies target ads in many different ways, including:

- Tailoring ads on search sites based on what is being searched for (this could either take the form of text links, videos and/or images);
- Using information from browsing history (sites visited, searches made) to better target display ads on other sites;
- Using information from users' profile on social networks and what things they have "liked" or shared;
- Simply using the content of the website/app to draw inferences about what ads a user may be interested in ("contextual ads"); and
- Sending targeted e-mails based on what products a user has searched for.

### What impact could GDPR have?

Figure 1 Key features of GDPR



GDPR will require telecoms operators to be even more vigilant about preventing data breaches. This will impose extra costs on them<sup>11</sup>, such as higher costs relating to data security, management of consent, and the challenges of fulfilling data subject right requests<sup>12</sup>.

They may also be even more cautious about venturing into advertisement services, as they now also have to be concerned about complying with GDPR. It is less clear that GDPR will affect the ability of telecoms operators to optimise network performance, tailor customer tariffs<sup>13</sup> and sell insights based on aggregated data.

<sup>11</sup> The following article suggests that the costs of implementing GDPR for the telecoms industry are somewhere in the middle of the range relative to other sectors. It estimates that the costs for the technology & telecommunications sector will be £20m. (<https://www.consultancy.uk/news/15101/gdpr-compliance-to-cost-ftse100-firms-15-million-banks-face-largest-bill>)

<sup>12</sup> For example, individuals will be able to request that firms provide them with a copy of their personal data.

<sup>13</sup> Although this may depend on the extent of profiling and/or automated decision-making that leads to differential pricing, which could thereby result in an adverse effect on the subscriber.

This is because these types of data usage do not rely on personal data and/or are needed to deliver the services requested by the subscriber (they would be expected to satisfy the so called “purpose limitation” criterion<sup>14</sup>). In summary, the potential impact for most operators is likely to be on possible future revenue streams rather than existing revenues - unless they face a serious data breach.

The impact of GDPR on the large internet players is unlikely to be uniform, as GDPR is more likely to have an impact on large internet players that heavily rely on ads as a source of revenue<sup>15</sup>. Therefore, players such as Google and Facebook are likely to be more concerned than players such as Apple who do not rely on advertisements as a source of revenue. The number of ads shown won't change, but companies might not be able to target them as accurately as before depending on: (i) how exactly “purpose limitation” is interpreted; (ii) what type of information falls into the scope of GDPR's definition of “personal data”; and (iii) the large internet players' ability to get their customers to provide their consent.

### Personal data and purpose limitation

Under GDPR, “personal data” is quite a broad term that includes any information that can identify a person, such as their name, photo, email address, IP address, bank details, posts on a social networking site, medical information and biometric data.

Firms do not need consent to process personal data if this is required to provide the service users have requested. As a result, some types of advertisements are likely to fall into a bit of a grey area. For example, industry commentators have argued that location-based ads within Google Maps may fall within the scope of “purpose limitation” (i.e. they are consistent with the original purpose for which the data was collected) and so would not require consent<sup>16</sup>, just an acceptance of the terms and conditions. Put another way, it could be argued that location-based ads are part of the service provided by Google Maps.

The types of ads likely to be most affected are those that rely on information that is i) clearly classified as personal data and ii) has been collected by a party other than the publisher hosting the ads<sup>17</sup> - for example, an ad based on personal data collected by Google, but posted on a non-Google website through Google's ad network. Under such circumstances, consent would be required. This could be challenging because the publisher would have no direct relationship with the user to whom the data relates. Contextual ads that do not rely on personal data should be least affected e.g. an advert for BT Sport on a tennis website.

As Google has reported that most of its ad revenues do not rely personal data<sup>18</sup>, internet players with business models such as Google's, may be relatively less affected than players with business models closer to Facebook's<sup>19</sup>. The latter, may face tougher challenges in relation to supporting ads that are targeted on the basis of a users' personal characteristics or preferences<sup>20</sup>.

<sup>14</sup> Personal data has to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

<sup>15</sup> Google and Facebook were already facing lawsuits totalling £6.7bn on the day GDPR came into force (<https://www.theinquirer.net/inquirer/news/3033111/google-and-facebook-rack-up-gbp67bn-in-gdpr-lawsuits-on-day-one>).

<sup>16</sup> See [https://pagefair.com/blog/2017/gdpr\\_risk\\_to\\_the\\_duopoly/](https://pagefair.com/blog/2017/gdpr_risk_to_the_duopoly/)

<sup>17</sup> For example, most news websites will host advertisements based on data collected from elsewhere.

<sup>18</sup> Google's CEO has stated (“First of all, it's important to understand that most of our ad business is search, where we rely on very limited information — essentially what is in the keywords — to show a relevant ad or product.”) <https://www.cnbc.com/2018/04/23/google-sundar-pichai-on-gdpr.html>

<sup>19</sup> We note nevertheless that there are signs that GDPR is having some effect – e.g. Google recently announced that it had stopped using emails sent through Gmail as a source of information.

<sup>20</sup> This is especially true for ads that rely on “special categories” of data, including ethnicity, religious beliefs, political affiliation and sexual orientation, as more stringent rules apply to such types of data under GDPR.

## Encouraging consumers to give their consent

GDPR has set more stringent requirements on how firms can gain consent, although exactly what strategies are permitted under GDPR is likely to be a key area of contention. Importantly, service cannot be withdrawn from users who do not consent to their personal data being used for other purposes as this approach would mean any consents gained are not truly 'freely given' and therefore invalid.

Large internet players have invested a lot of thought into how they can get such consent. We know from behavioural economics that small prompts can 'nudge' users to the desired outcome when it comes to agreeing to terms and conditions or offering consent<sup>21 22</sup>. Both the effectiveness of the strategies deployed and their compatibility with not only the letter, but also the spirit of GDPR, remains to be seen.

## Conclusion

The impact of GDPR on existing revenues streams may not be a significant concern for most telecoms operators unless they face a serious data breach. It can however reduce the attractiveness of some business models to monetise data in future – notably targeted/personalised advertising. The new regulation is likely to have greater repercussions for internet players, the business models of which are reliant on using user data. Not all such business models rely to the same extent on the use of personal data. And, in any case, companies using personal data have already been under pressure to be more transparent about how they use personal data (as illustrated by the recent Cambridge Analytica case).

An important driver of the ability of large internet players to be able to continue to generate value from their business models, will be the maximisation of users that continue to use the 'free' services. In conventional one-sided business models, the provider can generally withdraw a service if a user does not pay. When payment takes the form of access to personal data, or consent for its use, this option is not available. Nevertheless, large internet players have significant knowledge, based on their own insights and bolstered by findings from behavioural economics, of how to nudge users towards the outcome they seek. And whilst a reduction in the large internet players' ability to target ads could reduce their revenues, GDPR could also potentially make it more difficult for smaller players to enter or expand in these markets, if the costs of compliance with GDPR are significant and/or if they find it more difficult to gain consent<sup>23</sup>.

<sup>21</sup> See for example "Thaler (2009) - Nudge: Improving decisions about health, wealth and happiness"

<sup>22</sup> Frontier has previously produced an article on how firms may use Behavioural Economics to encourage consumers to share their data ([https://www.frontier-economics.com/documents/2018/01/frontier\\_data-protection.pdf](https://www.frontier-economics.com/documents/2018/01/frontier_data-protection.pdf))

<sup>23</sup> See for example <https://www.forbes.com/sites/jonmarkman/2018/05/22/gdpr-is-great-news-for-google-and-facebook-really/#25d8e34e48f6>



Tom Ovington

+44 (0) 207 031 7179

tom.ovington@frontier-economics.com



Jose Maria Rodriguez

+34 91 343 2355

jose.maria.rodriguez@frontier-economics.com