SLAUGHTER AND MAY/

CLIENT BRIEFING

JULY 2021

THE CONSEQUENCES OF PAYING WITH DATA

A version of this briefing first appeared in the Privacy Laws & Business UK Report, Issue 116 (July 2021)

Never has the use of data had a bigger impact in our lives as consumers; from helping us decide where to eat based on our previous experiences and giving us tailored offers at our favourite supermarket, to being able to obtain a mortgage quote at the click of a few buttons and ensuring we have quick access to GPs.

Many companies that offer services based on the use of our personal data do so without requiring payment in the traditional sense. Indeed, we can navigate our way through the country, find out our credit score and stay in touch with our friends online without ever encountering a paywall. However, we are often sharing our personal data instead, sometimes more or less unwittingly.

The monetary value of this exchange (for example in terms of the marketing opportunities our data presents) has long been acknowledged, but how to rectify this imbalance and somehow compensate or incentivise the individual is not as simple as it may initially appear. In this briefing we explore the intended and unintended consequences of 'paying with personal data'.

1. Paying with personal data

There is a growing concern that individuals are losing control over their data as a result of the shift from traditional payment mechanisms to 'paying with their data', and particularly when accompanied by compensation or incentives (e.g. discounts on products or vouchers). Examples include mobile phone apps which might appear to be "free" at first glance, but have language in their terms and conditions and privacy notice that permits the collection and commercialisation of personal data generated on the users' device; insurers providing discounts to policy holders who share data on their driving behaviour and supermarkets that collect information about customers' shopping behaviour by way of loyalty cards (through which the customers earn discounts).

We discuss below some of the specific concerns commonly raised in relation to paying with data and explore what the future may hold for them.

(a) Transparency and lack of control

Many individuals simply do not understand what happens to their information once they have duly completed the "*required fields" to access the tool or app they want. Although the UK GDPR places organisations under an obligation to explain to individuals how their data will be used in a way they will understand, there is a widely reported disconnect between the transparency obligations included in privacy legislation and consumers' understanding (see the *World Economic Forum White Paper, Redesigning Data Privacy: Reimagining Notice & Consent for human-technology interaction, p7*). For example, a New York Times investigation in 2019 emphasised this gap: it analysed 150 privacy policies from popular websites and apps and found that the majority required a college level reading ability, above that of over half Americans. Without being able to understand the privacy information they are provided, individuals are unclear about to whom and where their information is going, which in turn is likely to result in a loss of control. Adding a financial incentive of some sort to the mix is, one might argue, even less likely to encourage individuals to fully read a privacy notice and/or make informed choices.

(b) The absence of consumer protection

There have also been longstanding concerns that by exchanging information rather than paying for a service, consumers miss out on protections that would be afforded to them by law if they had paid (*see for example the European Commission press release (2017) following an analysis of EU consumer and marketing rules*). For example, under current consumer protection legislation a consumer that makes an online purchase by debit card has the

right to their money back if they return the product, yet no such right is available for those that provide their personal data in equivalent exchange.

(c) The potential for unfairness and discrimination

It has been suggested that financial incentives for sharing data put less wealthy individuals at a disadvantage. Similarly, some argue that the dichotomy between those who can pay obtaining greater rights and those who cannot pay being denied those same rights is being entrenched by the specific devices individuals use. Apple has long been marketing itself on the basis of its privacy credentials and has recently gained substantial publicity in light of its move to give users greater control over the apps that track them. However, Apple's devices occupy a premium position in the market and tend to cost significantly more than the vast majority of handsets running Google's Android system. As with financial incentives for sharing data, there is an argument that this could create a 'privacy divide' favouring the wealthy.

2. Recent developments

Although, at this moment in time, there doesn't appear to be one single solution to the challenges outlined above, there are developments in a number of fields that could help, including:

(a) Enforcing existing privacy legislation

If a privacy notice doesn't clearly and intelligibly explain what happens with an individual's data, or if an individual isn't presented with a genuine choice when consenting to the use of their data, then data regulators can, and do, bring enforcement action. GDPR enforcement action across the EU has consistently increased over the last few years, with a number of fines being issued for breaches of the transparency requirements and invalid consent (e.g. the French data regulator's fine of 50m euros against Google).

However, there is an unresolved question around the extent of personal responsibility – whose fault is it where a customer fails to read a privacy notice? This is not something we have seen tested by the Information Commissioner's Office (ICO) in its GDPR enforcement actions to date (which in the last 3 years have focused mainly on data security failings). Where an organisation tailors comprehensive privacy information to their audience and provides it in a clear and timely fashion, i.e. complies with its UK GDPR obligations, it is hard to see that an individual's failure to engage can be viewed as non-compliance by the organisation. Conversely, it is arguable that adding a financial incentive (such as a time-limited discount in exchange for sharing personal data) alters this analysis and could be viewed as unfair.

(b) Using technology to give individuals control

New or enhanced products and services aimed at giving individuals greater control over their data are continuously being developed, with many businesses keen to differentiate themselves from their competitors on the basis of the level of data protection they offer. Examples include the 'DuckDuckGo' internet search engine which distinguishes itself from other search engines by not profiling its users and by showing all users the same search results for a given search term. Or the 'Gener8' free web browser which lets internet users choose whether to share their data and be rewarded if they do so - and claims it can enable publishers to monetise users who would otherwise be using ad-blockers. Big tech clearly has an important role to play within this as well, from developing leading privacy practices to engaging with regulators. For example, it has been reported that Google is enhancing the privacy protection of Android users who want to make it harder for advertisers to track users as they move between apps.

Data trusts are another potential solution. The ICO describes them as "a legal structure that allows for independent third-party stewardship of data. […] they facilitate sharing between multiple organisations, but do so in a way that ensure that the proper privacy protections and other relevant protections are in place" (*ICO 2019 response to the Digital Competition Expert Panel's review of the State of Competition in the Digital Economy*). Data trusts were mentioned in the UK's recent Data Strategy and the UK's 2017 AI Review and the government has invested in research in this area as well, so we can expect to hear more about them going forwards.

(c) Civil action

The issue of lack of control over data has, unsurprisingly, been picked up on by consumer groups and privacy activists, as can be seen in the highly publicised court case of Lloyd v Google. This was a collective action brought by Mr Lloyd, the former chairman of Which?, on behalf of a potential class of up to 4m Apple iPhone users. It has at its centre questions of data value, (perceived) loss of

control by the relevant affected individuals, and who should be entitled to reap the rewards of any data monetisation. The Supreme Court's judgement is awaited.

(d) Consumer protection

Some EU data regulators are looking for help beyond existing data privacy rules. For example, the Dutch regulator commented in May this year (in the wider context of the proposed EU Digital Services Act) on the issue of paying with data and the 'privacy divide' it may create. It has been suggested that Dutch law should be amended to require a two week window after 'purchase', during which any personal data received as 'payment' cannot be shared with third parties and must be returned if the consumer changes their mind and returns the product. In addition, the regulator would like to see an obligation on companies that collect data as payment to make it clear to consumers what the price of the product or service would otherwise be if no data was shared.

More generally, the need for consumer protection for those paying with their personal data has been recognised by the EU in its 'New Deal for Consumers' Directive which EU Member States have until November 2021 to implement. The Directive amends a number of key existing EU consumer laws so they will apply to 'free' digital services provided in exchange for consumers' personal data and gives certain additional consumer protections, including a 14 day cancellation right. It remains to be seen how this cancellation right will operate in practice, whether consumers will be able to recover their personal data if they opt to cancel and what, if anything, the UK will do to replicate this 'New Deal'. For now, it does not appear to be a priority for the UK government.

(e) Reforming existing laws in the UK

Post Brexit, the UK government has made various references to reforming existing legislation such as the UK GDPR in order to pursue data opportunities and help drive growth and innovation – whilst still maintaining high standards of data protection (*see for example the UK's National Data Strategy*). There are also various legislative proposals and potential areas for reform or future development that may directly or indirectly address some of the concerns identified in this briefing. Examples include the Competition and Markets Authority's (CMA) refreshed Digital Markets Strategy that now encompasses the recommendations of the Furman Review and the Centre for Data Ethics and Innovation's (CDEI) recent report on 'Active choices' which considers how digital interfaces can be designed to empower users to make active choices about their privacy settings.

There are also a number of EU proposals which the UK is considering replicating, such as the e-Privacy Regulation and the requirements around cookie walls or the EU's Digital Services Act package. Some of these proposals are more advanced than others but for many, it is still unclear when and how they will be implemented in the UK.

(f) Big tech and competition

Big tech is often at the centre of any discussion around data usage, transparency and individuals' control. Data regulators have a long history of engaging with big tech, both collaboratively and, in some EU jurisdictions, on a more contentious basis. Regulators in other fields are also getting involved. For example, as we discuss in our Regulating Digital Hub, competition regulators are increasingly interested in how big tech is using personal data and the impact such use may have on competition, and ultimately harm individuals (see for example the CMA's January 2021 paper on 'Algorithms: how they can reduce competition and harm consumers'). This has resulted in a plethora of reports, recommendations and reform proposals from the various regulators. Helpfully, some of the regulators are combining resources, such as the CMA, the ICO, and Ofcom who have established a Digital Regulation Cooperation Forum (with the Financial Conduct Authority joining as a full member in 2021) to ensure a greater level of cooperation around the regulation of online platforms. This in turn will help organisations looking for guidance.

3. The way forward

As is clear from the number of initiatives, reports and reform proposals mentioned above, there is significant activity in this area. Further clarity on how the various proposals interrelate, and how the regulators will guide and enforce, would be welcome. It will also be interesting to see to what extent the UK may end up diverging from the EU and the consequences this may then have on international data flows and the continued recognition by the EU of the UK as "adequate".

In the meantime, businesses should keep focussing on getting the fundamentals of data privacy right. The ICO has repeatedly made clear its views on the importance of control and choice (and transparency) for individuals. For example, when commenting on the Memorandum of Understanding

and May 2021 joint statement between the ICO and the Competition and Markets Authority, Elizabeth Denham, outgoing Information Commissioner, said that "Modern data protection regulation [...] provides a roadmap for companies to share personal data responsibly and to innovate in a privacy friendly way. It also requires that people have control and understanding of how their data is used, which is crucial for building the public trust that underpins successful digital markets."

Although lacking a clear regulatory trajectory, the focus on paying with data is not going away any time soon. Only last week the Dutch court allowed a significant group action to proceed against Facebook, with one of the claims being for 'unjust enrichment' on the basis that the tech firm misled users into believing the service was free, when they were essentially 'paying with their data'.

CONTACT

ROB SUMROY
PARTNER, CO-HEAD OF DATA PRIVACY
T: +44 (0)20 7090 4032
E: rob.sumroy@slaughterandmay.com

CINDY KNOTT
SENIOR PSL & HEAD OF KNOWLEDGE – DATA PRIVACY
T: +44 (0)20 7090 5168
E: cindy.knott@slaughterandmay.com

LUCIE VAN GILS
DATA PRIVACY LAWYER
T: +44 (0)20 7090 3560
E: lucie.vangils@slaughterandmay.com

BRYONY BACON
DATA PRIVACY PSL
T: +44 (0)20 7090 3512
E: bryony.bacon@slaughterandmay.com