What is the true 'loss' to individuals in competition cases?

Claire Saunders and **Jenai Nissim** of HelloDPO Law discuss the *Gormsen* case which raises the question whether consumers should be compensated for the personal data that Facebook monetises for advertising.

When the Supreme Court dealt a substantial blow to collective proceedings for data protection claims in *Lloyd v Google*,[1] surely we all knew that would not be the end of the story? Since then, there has been action in the courts on data protection related cases and now a case in the Competition Appeal Tribunal (CAT) has reason to make data protection professionals sit up and pay attention!

The claim

In early 2022, Dr Liza Lovdahl Gormsen applied to commence opt-out collective proceedings (this is where the class members automatically become part of the claimant class unless they actively opt out) under the Competition Act 1998 against Meta Platforms Inc., Meta Platforms Ireland Limited and Facebook UK Limited (collectively described as Meta below).

The claim against Meta is for approximately £2.2bn (plus interest) and is made on behalf of a class of approximately 45 million individuals - individuals in the UK who had a Facebook account and accessed it at least once between 11 February 2016 and 31 December 2019 inclusive.

In February 2023, the CAT handed down a judgment in relation to Dr Lovdahl Gormsen's application for certification of the proceedings, granting a stay of six months to allow the claimant representative to better clarify a "new and better blueprint for the effective trial of the proceedings" for the reasons discussed below.

Unlike claims under data protection legislation, in the CAT, there is a specific regime for collective proceedings which allows a representative who is certified by the CAT to bring a claim on behalf of a class of claimants, without the need to individually identify them. A claim has to be certified by the CAT in order to proceed as a collective action. The regime has been in existence since 2015 and it was initially unclear how much the regime would be used; however, it has grown in popularity thanks to the seeming eagerness to certify these types of claims. In a recent case involving Mastercard, the Supreme Court is considered to have significantly lowered the bar for certification, opening the door to these types of claims, holding (amongst other things) that the method of distributing damages does not have to reflect the individual claimants' losses, a sharp contrast with *Lloyd v Google*, where the Supreme Court, although seeing no reason why monetary remedies could not be claimed in a collective action, considered that the difficulties lie in the fact that an individualised assessment of loss would normally be needed. The court considered, however, that a collective claim might be appropriate where the entitlement can be calculated on a basis which is common to all of the class members (e.g., they were wrongly charged a fixed fee) or where the loss can be calculated without reference to the loss suffered by individual class members.

The judgment in question does not deal with the strength of the parties' arguments in the central case but considers whether the claimant representative has presented a methodology for establishing loss on a class wide basis – a means by which the loss is common to the class, an important element in order to allow claims to proceed collectively. This is known as the "Pro Sys" test. It is necessary for this test to be satisfied in order for a claim to continue.

Factual background

Meta provided its services to users of Facebook as quoted in the judgment: "[We] don't charge you to use Facebook or the other products and services covered by these Terms. Instead, businesses and organisations pay us to show you ads for their products and services. By using our Products, you agree that we can show you ads that we think will be relevant to you and your interests. We use your personal data to help determine which ads to show you."

Meta used personal data submitted by users to determine which adverts might be relevant to them. They did not sell personal data to advertisers, but offered advertisers the ability to show adverts to a relevant audience without sharing information that personally identifies users.

The allegations

The claimant representative argued that Facebook was not provided free of charge, but was paid for with:

- personal data provided by users explicitly (such as name and contact details),
- personal data provided implicitly (such as contacts, browsing history, private messages, behavioural patterns),
- personal data obtained by or via third party websites and application shared with or obtained by Facebook (such as browsing history, Internet usage, census data, health data), and/or
- sensitive data (such as individuals' racial or ethnic origin, political opinions, religious beliefs, sex life and health).

This personal data was then monetised and exploited by Meta with no payment being provided to users.

The claim made three main allegations as to how Meta exploited its dominance in breach of competition law, all of which relate to Meta's use of personal data:

1. Imposing an **Unfair Data Requirement**: Meta collected personal data

beyond what was needed for the provision of a social media network, which was disproportionate and/or not necessary;
2. **Unfair Price allegations**: Meta demanded an unfairly high "price" or "payment in kind" (in terms of the personal data required) for use of the platform and that on the other hand, by only providing the social media network in return, it paid an unfairly low "price" for the personal data; and
3. **Unfair Trading conditions allegations**: individuals who wanted to use Facebook (allegedly the dominant social media network) were unable to avoid the terms and conditions imposed by Meta, which were excessively long and complex, hard to understand and subject to frequent unexplained changes. Additionally, Meta failed to sufficiently explain what personal data was collected and how it was used and furthermore, decreased privacy protections over time with its increasing dominance.

The CAT decision

Having considered the claim, the CAT concluded that the claimant had failed to put forward a methodology for establishing a "loss", to the individuals whose personal data was the subject of the class action, on a class-wide basis and instead, the claim was mostly focused on the monetary value derived by Meta for the use of the personal data (an unacceptable approach).

The CAT found, in relation to the Unfair Terms and Conditions claim, that the effect of the alleged misleading statements in Meta's terms and conditions was likely to be different for different individuals and as such the CAT expressed concern as to whether it was suitable for collective proceedings. The CAT also expressed doubts that this claim could be made under competition law.

In respect of the Unfair Price allegations, the CAT accepted that "the difference between the price actually charged and the price that should have been charged" represented the measure of loss to the claimants.

However, the methodology produced for assessing an excessive price (and so potentially an abusive price) had not been sufficiently set out. The CAT also commented on the fact that the claimant's case does not fall squarely within the current case law, which could pose problems.

What's next?

Having found the methodology lacking, the CAT has given Dr Lovdahl Gormsen six months in which to conduct a "root and branch" re-evaluation of it. The CAT reasoned that the need for access to justice required them to let the claimant "have another go". Interestingly Meta did not apply for the claim to be struck out (dismissed) and the CAT did not make the order itself, even though they were highly critical of what was put forward by the claimant representative.

Whilst not assessing the merits of the central case, the CAT did make various comments throughout the judgment which give the impression that the case may be problematic in several areas.

What can we learn from this case as DP professionals?

Whilst the case itself is unlikely to shed light on data protection issues *per se*, there is no doubt that we should be keeping an eye on the progress of this case in so far as it links strongly back to the notion of quantification when claiming "loss" for misuse of personal data. If the claim is successful, it would certainly require a change in practices by Meta from a personal data use perspective and given the size of the class, the impact would not be an insignificant event even for Meta. Furthermore, those providers of similar social media platforms/apps that have a dominant position in their market will no doubt be watching with interest.

If Dr Lovdahl Gormsen is successful in re-working the methodology for loss and is eventually successful at trial (although it appears this is far from certain), claimants may start to more carefully weigh up the relative merits of competition cases versus action under data protection legislation in situations where the defendant seems to have a dominant position.

The CAT is familiar with and seemingly sympathetic towards collective action proceedings and so may be more appealing to claimants if they have reason to believe they can successfully plead competition law infringements. It is also the case, as mentioned above that the competition regime views the distribution of damages more flexibly than under the procedure used in proposed collective claims based on data protection legislation/misuse of private information, which may mean a claim by collective action is more likely to be possible.

In *Lloyd v Google*, the court considered that it would be unlikely that a claim somewhat similar to this one, (involving assessing what a reasonable person would pay to use the personal data in question) could be pursued by means of collective action because of a requirement for individualised assessment of damages (where the approach of awarding "lowest common denominator damages" would lead to no award), although the court did suggest, elsewhere in the judgement, that it might be possible in some situations to have a two-stage process, to assess and rule on common issues and then proceed to individual assessment of damages.

If a methodology for loss can be established, perhaps it may also assist those trying to make data protection related claims in making their cases with regard to damage suffered (albeit maybe only for individual claims), which could encourage further claims.

It will also be interesting to see if Meta pushes the argument that the data processing was not excessive but was necessary to provide the services and if so, what the CAT makes of that argument. It is clear that (unlike the European Data Protection Board) the Irish Data Protection Commission has sympathy with this position stating in its press release in January 2023 (in relation to the fines levied against Meta Platforms Ireland Ltd) that "Facebook and Instagram services include, and indeed appear to be premised on, the provision of a personalised service that includes personalised or behavioural advertising" and that "in the view of the Data Protection Commission, this reality is central to the bargain struck between users and their chosen service provider, and forms part of the contract concluded at the point at which users accept the Terms of Service."

Finally, the reference made by the CAT to the possibility that there might

be grounds for a consumer protection based claim in relation to the alleged unfair terms imposed by Meta is intriguing; another possible avenue for cases which involve personal data? However, the CAT's comments that this type of case may not be suitable for collective action (given the different way in which the misleading statements by Meta would have affected the individuals) could put a stop to meaningful action on this front.

As readers will be aware, this case is not the only issue Meta is facing at the moment. With the Irish Data Protection Commission recently confirming that Meta Platforms Ireland Ltd unlawfully processed personal data in the use of targeted advertising (even though, as mentioned above, they took issue with this analysis by the EDPB), the risk of actions by data subjects is not going away any time soon.

It remains to be seen whether there could be an attempt at framing an action which might overcome the hurdles in *Lloyd v Google* (at the time of writing there is at least one ongoing attempt) and whether Dr Lovdahl Gormsen will manage to convince the CAT to let her proceed with this case. Watch this space!

REFERENCE

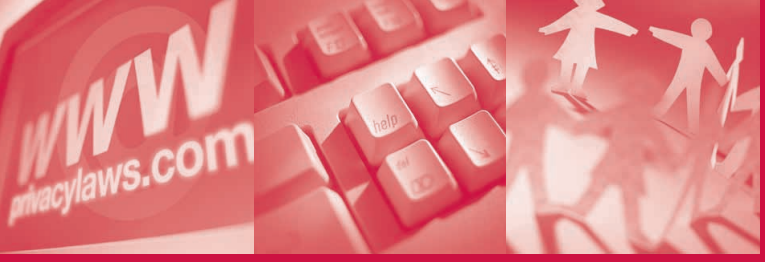
1 *PL&B UK Report* January 2022 p.1

AUTHORS

Claire Saunders is a Professional Support Lawyer, and Jenai Nissim is a Director and Co-founder of HelloDPO Law.
Emails: clairesaunders@hellodpo.com, jenainissim@hellodpo.com

INFORMATION

The CAT judgment of 20 February 2023 is at www.catribunal.org.uk/judgments/14337722-dr-liza-lovdahl-gormsen-v-meta-platforms-inc-and-others-judgment-cpo-application



ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Spot the difference: The DPDI (No. 2) Bill starts its legislative journey

Rebecca Cousin, **Lucie van Gils** and **Hilal Temel** of Slaughter and May look into the proposed changes which do not mark a radical change from the 2022 Bill.

For businesses across the UK and beyond waiting to see what a UK GDPR 2.0 might look like, the journey towards revised data privacy laws in the UK has begun (again). The Data Protection and Digital Information (No. 2) Bill (2023 Bill) was introduced in the

Continued on p.3

DP Bill receives House of Commons second reading

The Opposition criticises the government for not taking the opportunity to make a real change from the GDPR. **Laura Linkomies** reports.

The Data Protection and Digital Information (No. 2) Bill had its Second Reading at the House of Commons on 17 April. Several Labour MPs said that while they are largely supportive of the government's aims for a data reform, this Bill does not fulfil this objective.

Aspects that attracted many questions were the wide-ranging powers for the Secretary of State to approve codes of practice, and the ICO's

Continued on p.5

Issue 127 **MAY 2023**

UNITED KINGDOM
report

ISSUE NO 127 MAY 2023

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Rebecca Cousin, Lucie van Gils and Hilal Temel
Slaughter and May
Chris Pounder
Amberhawk Training Ltd
Edward Machin
Ropes & Gray
Victoria Hordern
Taylor Wessing
Madeleine Weber
Zscaler
Claire Saunders and Jenai Nissim
HelloDPO Law

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

AI White Paper proposes joint regulatory guidance

The UK government is investing heavily in AI, and is now trying to create an environment for AI to flourish. The much-awaited White Paper identifies however, some risks to human rights and privacy, for example the use of AI to generate deepfake pornographic video content, bias in assessing credit-worthiness of loan applicants, or intrusive collection of data through connected devices in the home. On a larger scale, the privacy law community needs to worry about disinformation generated and propagated by AI, and its impact on trust in democratic institutions and processes.

The consultation on the AI White Paper is now open for 12 weeks, until 21 June. This is the time to shape the future direction of AI in the UK – although regulation elsewhere will have an impact too (p.12). Cross-jurisdictional requirements mean that companies need to prepare AI compliance programmes now. Organisations can no longer claim they were not aware of the issues involved. The ICO has for some time been saying that AI is no longer a new concept, and it will therefore enforce data protection law on AI as vigorously as in any other field.

The White Paper will lack any statutory footing, and the government is not seeking to appoint a new regulator. While AI is a strategic priority for the ICO, as is empowering responsible innovation, the regulator says that it would welcome clarification on the respective roles of government and regulators in issuing guidance and advice as a result of the proposals in the AI White Paper. The ICO encourages the government to reach out to the Digital Regulation Cooperation Forum (DRCF) which consists of several regulators in this field, and where joint regulatory responses can be formulated.

In April, the Data Protection and Digital Information No. 2 Bill received its second reading in the House of Commons (p.1). The Online Safety Bill is at the Committee stage in the House of Lords, and the Digital Markets, Competition and Consumers Bill was recently introduced into Parliament (p.8). All this activity will keep DPOs, and us at *PL&B*, very busy. Join the debate at *Who's Watching Me?* our summer conference in Cambridge in July to hear from the new government home for data protection, the Department for Science, Innovation & Technology (DSIT, p.22), the ICO and other stakeholders. Register at www.privacylaws.com/plb2023.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Versions
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"The UK and International *PL&B* Reports have been my 'go to' resource for 20 years despite the wide choice of alternate resources now available. And have you tried the Annual Conference at Cambridge? I have seven IAPP certificates so a big IAPP supporter. But the *PL&B* Cambridge event each July, still knocks the spots off IAPP and other conferences!"

Derek A Wynne, SVP Privacy & Chief Privacy Officer, Paysafe Group

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 36th year. Comprehensive global news, currently on 180+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.