AN A.S. PRATT PUBLICATION
FEBRUARY-MARCH 2022
VOL. 8 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 2** **February-March 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [2] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.
LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2022 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR
Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Emilio W. Cividanes
Partner, Venable LLP

Christopher G. Cwalina
Partner, Holland & Knight LLP

Richard D. Harris
Partner, Day Pitney LLP

Jay D. Kenisberg
Senior Counsel, Rivkin Radler LLP

David C. Lashway
Partner, Baker & McKenzie LLP

Craig A. Newman
Partner, Patterson Belknap Webb & Tyler LLP

Alan Charles Raul
Partner, Sidley Austin LLP

Randi Singer
Partner, Weil, Gotshal & Manges LLP

John P. Tomaszewski
Senior Counsel, Seyfarth Shaw LLP

Todd G. Vare
Partner, Barnes & Thornburg LLP

Thomas F. Zych
Partner, Thompson Hine

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2022 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

UK Supreme Court Rules in Google's Favor in Data Privacy Group Litigation with Major Implications for Data Breach Cases

By Huw Beverley-Smith and Paige Izquierdo*

The authors of this article summarize a judgment handed down by the UK Supreme Court, which is potentially one of the most significant and anticipated data privacy judgments to date.

The UK Supreme Court has handed down a judgment in *Lloyd v. Google LLC*,[1] which is potentially one of the most significant and anticipated data privacy judgments to date.

BACKGROUND

This long-running litigation in the English courts related to Google's Safari workaround which, it was alleged, in 2011-12 bypassed privacy settings and allowed Google to track the internet activity of millions of Apple iPhone users and use the data collected in this way for commercial purposes without the users' knowledge or consent. This allegedly allowed Google to collect or infer information relating to users' internet surfing habits and location, interests, age, gender and other personal information – and then offer the group labels to subscribing advertisers for targeted marketing.

In 2012, Google agreed to pay a civil penalty of US$22.5 million to settle charges brought by the U.S. Federal Trade Commission based upon the allegation and subsequently US$17 million to settle consumer-based actions brought against it in the United States.

In England and Wales, three individuals sued Google in June 2013 making the same allegation and claiming compensation under the Data Protection Act 1998 ("DPA 1998") and under the tort of misuse of private information. Following a dispute over jurisdiction, those claims were settled before Google had served a defense.

In the present action the claimant, Mr. Lloyd, was not just claiming damages in his own right. Rather, he claimed to represent every one of the four million or so iPhone users resident in England and Wales at the relevant time whose data was obtained by

* Huw Beverley-Smith is a partner at Faegre Drinker Biddle & Reath LLP advising customers and suppliers on a wide range of international transactions and regulatory issues, including privacy and cybersecurity, technology, telecommunications and business process outsourcing, services agreements, intellectual property ownership and licensing. Paige Izquierdo, a trainee solicitor at the firm, assists clients with actionable guidance on a range of corporate matters. Resident in the firm's London office, the authors may be contacted at huw.beverley-smith@faegredrinker.com and paige.izquierdo@faegredrinker.com, respectively.

[1] [2021] UKSC 50 (November 10, 2021).

Google without their consent. Unlike the United States (and other jurisdictions such as Canada and Australia), class actions are not generally permitted, other than in limited circumstances in specific areas.

Mr. Lloyd sought to overcome this difficulty through the use of the representative procedure. This allows a claim to be brought by one or more persons (as representatives of others) who have "the same interest" in the claim. Mr. Lloyd accepted that this procedure could not be used to claim compensation on behalf of other iPhone users if the compensation recoverable by each user would have to be individually assessed. He argued that such individual assessment was unnecessary since compensation could be awarded for "loss of control" of personal data without the need to prove that the claimant suffered any financial loss or mental distress as a result of the breach in the form of a "uniform sum" of £750 (just over US$1,000) with no need to investigate any circumstances particular to their individual case. Multiplied by the number of people whom Mr. Lloyd claimed to represent, this would produce an award of damages of the order of £3 billion (just over US$4 billion).

Because Google is a Delaware corporation, Mr. Lloyd needed the English court's permission to serve the claim form on Google outside the jurisdiction. Google challenged this on the grounds that the claim had no real prospect of success as: (1) damages cannot be awarded under the DPA 1998 for "loss of control" of data without proof that it caused financial damage or distress, and (2) the claim in any event is not suitable to proceed as a representative action.

UK SUPREME COURT JUDGMENT

The UK Supreme Court found for Google on the central issues as summarized below.

Potential to Claim Damages in a Representative Action Is Limited

Lord Justice Leggatt held that a representative action was a legitimate means of pursuing low-value claims relating to consumer rights. However, the potential for claiming damages in a representative action was limited by the compensatory nature of damages as a remedy at common law, given that damages typically require "an individualised assessment which raises no common issue and cannot fairly or effectively be carried out without the participation in the proceedings of the individuals concerned." This could not be achieved in a representative action.

A representative action could, however, have been used to establish whether Google was in breach of the DPA 1998 and, if so, seek a declaration that any member of the represented class who had suffered damage as a result of the breach was entitled to be paid compensation. Individuals would then go on to seek a damages award separately, through an individualized assessment on the basis of their own circumstances. While Mr. Lloyd's claim could have been advanced using this bifurcated (two-staged) process, this was not the approach adopted.

No Damages for Loss of Control

Lord Leggatt held that while it was possible for a representative action to include a claim for damages where the represented class members had all suffered the same loss, for example if they had all been overcharged the same amount, such situations were rare.

Mr. Lloyd attempted to argue that the class members had all suffered the same loss of a non-trivial breach of their rights as data subjects and that this had given rise to an entitlement to compensation for "loss of control" of personal data. He sought to establish new legal ground by extending the principles established in previous cases,[2] which are applicable to the assessment of damages for the tort of misuse of private information at common law to the assessment of compensation under Section 13(1) of the DPA 1998. He contended that "damage" goes beyond material damage and includes both distress, as decided in *Vidal-Hall v. Google Inc*,[3] and "loss of control" over personal data.[4]

The UK Supreme Court accepted that "loss of control" damages were available under the tort of misuse of private information (following *Gulati v. MGN*). However, it held that no such damages were available under the DPA 1998. Section 13 required "proof of material damage or distress whenever a data controller commits a non-trivial breach of any requirement of the Act in relation to any personal data of which that individual is the subject." The UK Supreme Court therefore rejected Mr. Lloyd's argument, finding it fundamentally inconsistent with the wording of Section 13, given that EU law (applicable at the time of the claim) did not provide a basis for giving a wider meaning to the term "damage" within that section than was given to the term by the Court of Appeal in the claim for misuse of private information in *Vidal-Hall v. Google*. Section 13 could not reasonably be interpreted as conferring a right to compensation on a data subject for any non-trivial contravention by a data controller without requiring the data subject to prove (i) the contravention, and (ii) that the contravention caused material damage or distress to the individual concerned.

Since the acts and omissions giving rise to the claims occurred in 2011 and 2012, they pre-dated the EU General Data Protection Regulation ("GDPR") and were governed by the UK DPA 1998, which implemented the preceding EU Data Protection Directive. While the parties referred to the GDPR the UK Supreme Court refused to take this into account in interpreting the relevant provisions. Nevertheless, Section 13 of the DPA 1998 and Article 82 of the GDPR (which sets out the rights of data subjects to compensation and the liabilities of data controllers) are similar in principle. Therefore, a similar outcome can be expected in future cases under the UK GDPR.

---

[2] Notably *Gulati v MGN Ltd* [2017] QB 149).

[3] 2016.

[4] Paragraph 108.

The Need for Individualized Evidence of Misuse

The UK Supreme Court found that even if "loss of control" damages had been available under Section 13, a representative action would not have been permissible because "it would still be necessary to establish the extent to the unlawful processing in his or her *individual* case."

The following factors were given as examples of necessary considerations in quantifying the damages (if any) to be awarded:

- The period of time during which Google tracked the individual's internet browsing history.
- The quantity of data that was unlawfully processed.
- Whether any of the information unlawfully processed was of a sensitive or private nature.
- The use made by Google of the information and the commercial benefit (if any) obtained by Google from that use.

The Claim for the "Lowest Common Denominator"

Mr. Lloyd claimed that it was possible to identify an "irreducible minimum harm" suffered by each member of the class for which a uniform sum of damages could be granted, (termed the "lowest common denominator" of all the individual claims). Even on the assumption that the persons represented would not be prejudiced individually by a representative claim for only the minimum part of the compensation which the individuals could potentially claim, the UK Supreme Court took the view that such an approach was problematic. If no individual circumstances were taken into account, then the facts alleged would be insufficient to establish that *any* member of the class was entitled to damages. That would be the case even if it was unnecessary to prove any material damage or distress to the individual.

Facts Common to Each Individual's Case

The UK Supreme Court held that the facts alleged against Google generically could not establish that any given individual would be entitled to compensation. To establish an individual's entitlement to damages, it would need to be shown, as a minimum, that there was unlawful processing relating to that particular individual. It was insufficient simply to establish that each claimant was a member of the class by showing that the individual concerned had an iPhone running the relevant version of the Apple Safari internet browser which, at the relevant time, was participating in Google's DoubleClick advertising service.

If there was any form of "damage" within Section 13, such damage could not be characterized as more than trivial. What gave the claim the appearance of substance

was the allegation that Google secretly tracked the internet activity of millions of Apple iPhone users for several months and used the data obtained for commercial purposes. But, the UK Supreme Court held, the claimant was seeking to recover damages without attempting to prove that this allegation was true in the case of any particular individual and therefore could not cross the threshold for an award of damages. This was because the claimant had, in order to bring the claim in a representative capacity for damages assessed from the bottom up, deliberately chosen not to rely on any facts about the internet activity of any individual iPhone user beyond those facts which brought then within the class.

User Damages on a Lowest Common Denominator Basis

The UK Supreme Court also rejected claims for damages awarded on a user basis – the fee which each member of the class could reasonably have charged or would have been agreed in a hypothetical negotiation. It stated that the object of an award of user damages is to compensate a claimant for the wrongful use of an asset protected by the right infringed. The starting point for the valuation exercise is to identify the extent of the wrongful use. Only then can an estimate be made of what sum of money could reasonably have been charged for that use or, put another way, for releasing the wrongdoer from the duties which it breached in the wrongful use that it made of the asset.

In Mr. Lloyd's claim, this could have been achieved by assessing the hypothetical fee negotiable for a license to place the DoubleClick Ad cookie on an individual user's phone as a third-party cookie and without releasing Google from its obligations not to collect or use any information about that individual's internet history. The UK Supreme Court took the view that such a license would be "valueless, and that the fee which could reasonably be charged or negotiated for it would accordingly be nil."

In summary, the UK Supreme Court did not grant Mr. Lloyd permission to serve proceedings against Google outside the jurisdiction of the courts of England and Wales, effectively bringing his claim to a close.

IMPLICATIONS

This is a very significant decision for Google, not least because of the number of data subjects and potential damages involved. It has broader implications for all data controllers, particularly when faced with potential claims resulting from data breaches. Claimants frequently assert that loss of control over their personal data is sufficient in and of itself, without setting out details of any damage in the form of financial loss or distress. These claims are now far less likely to succeed, since asserting breach of the Data Protection Act 2018 would seem to be extremely challenging.

Further, following an earlier English High Court decision in July 2021 in *Warren v. DSG Retail Ltd*, the scope of claims based on breach of confidence, misuse of private

information and negligence (which are often bundled together with claims for breach of the GDPR and the UK data protection legislation) have also been significantly limited. Data controllers obviously continue to have significant potential liabilities for data breaches which cause financial loss or some form of distress, but there is some comfort that the mere fact of a breach will not necessarily result in automatic payouts.

KEY TAKEAWAYS

- A representative action may be brought for claims of breach of data protection legislation, but only to establish liability. Any damages must be dealt with separately through a group action or individual claims.
- Damages are not available for mere "loss of control" of personal data following a non-trivial breach of the Data Protection Act 1998, even where there has been a misuse of private information. Damages can only be awarded if the data subject has suffered some form of material damage, such as financial loss or distress.
- If loss of control damages were available, Mr. Lloyd's claim could not have been brought as a representative action as it would still have been necessary to assess the extent of the alleged misuse of data in each individual case.