Legal and Economic Analysis of Personal Data - Related Collective Actions in the UK

by Peter Davis, Louise Freeman, Samid Hussain and Kate Scott[1]

Introduction

Businesses store and process vast amounts of personal data. When management of that data allegedly goes wrong, litigation can follow. Recently, a number of significant collective actions related to data have surfaced in the UK, including those involving Google[2], YouTube[3], Marriott[4], Morrisons Supermarkets[5], British Airways[6] and easyJet[7].

Data related collective actions can generally be divided into two broad categories: (i) "unauthorized use of personal data" cases, where the firm controlling personal data allegedly uses it in an unauthorized manner; and (ii) "unauthorized access to personal data" cases where a third party (e.g. hackers) improperly accesses private data for malicious reasons. This article discusses some of the key legal and economic issues that arise in matters involving the unauthorized use of, or unauthorised access to, personal data in the UK[8].

Data protection laws in the UK

"Personal data" can refer to diverse information types. The EU's General Data Protection Regulation (GDPR), which was implemented in the UK and supplemented by the UK Data Protection Act of 2018 (DPA 2018),[9] classifies personal data as any information relating to an identifiable individual. Examples of personal data include names, email addresses, financial information, health data, biometric and genetic data, data revealing racial or ethnic origin, and data about criminal convictions or offences. The form of personal data can vary and may include private photographs or videos.

Inter alia, the GDPR requires that "personal data must be collected for one or more specified and legitimate purposes"[10], and that it "must be processed lawfully, fairly, [and] in a transparent manner"[11]. The GDPR also requires firms to store personal data for "no longer than necessary"[12], and to take "appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, and damage to, personal data, to ensure a level of security appropriate to the risk"[13].

When a firm does not meet its GDPR obligations, the GDPR provides the aggrieved person(s) the right to compensation for both "material" and "non-material" harm, including distress,[14] unless the controller or processor "proves that it is not in any way responsible for the event giving rise to the damage"[15]. In each case, damages as a matter of English law are designed

to put claimants in the same position they would have been had the breach not occurred. The GDPR notes, in its recitals, that "*a personal data breach may … result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*"[16] Thus the categories of damage are potentially broad. A point being actively contested in the English Courts is whether a data subject can claim damages for "loss of control" of personal data, as we discuss further below.

Means of bringing collective claims in the UK

There are two principal means of bringing collective claims in personal data–related matters in the UK:

• A common route is a **Group Litigation Order** (GLO), which is brought on an "opt in" basis, where multiple claims give rise to "common or related issues". While there is a trial of common questions of fact or law (e.g., whether there was a breach of relevant legislation), the amount of damages is assessed for each claimant. For example, the claimants have used a GLO in *British Airways*.

• Alternatively, a **Representative Action** (RA) is brought on an "opt out" basis. Historically, RAs have been less common than GLOs since the representatives and the represented class are required to have the "same interest", which is a more stringent test than "common or related issues" for a GLO. However, recently the Court of Appeal (CoA) decision in *Lloyd v Google* suggested that RAs may prove a feasible way to launch a claim despite the "same interest" restriction. If the Supreme Court agrees with the CoA, *Lloyd v Google* may encourage further RAs on behalf of parties who have not necessarily suffered pecuniary loss or distress, but who are (according to the CoA) entitled to damages for "loss of control" over their personal information. The claim is structured to try to meet the "same interest" requirement by only seeking damages that represent the "lowest common denominator" of loss of control damages. Even so, the "opt out" nature of RAs means that actions involving substantial numbers of claimants are likely to result in damages claims for very significant aggregate amounts.

Beyond GLOs and RAs, other means of bringing collective claims include multi-claimant litigation. Companies may also propose their own remediation programmes to compensate affected data subjects. Looking ahead there may be an expanded role for class actions because of the EU Collective Redress Directive, albeit Brexit will mean that this will not directly impact the UK.[19] In addition, the UK government will need to decide whether to introduce legislation to provide for class actions similar to those currently available for competition matters.

Theories of harm in unauthorised use of, or access to, personal data matters

While the specifics of each case will determine the precise nature of claims, experience suggests that claimants in cases involving unauthorized use of personal data may take the position that privacy has an "intrinsic value" which is lost when personal data is misused or used without consent.[20] Thus, claimants may assign economic value to the integrity of private information, and argue for a common measure of damage, regardless of the nature of information at issue.

This view is consistent with the CoA's ruling in *Lloyd v Google* that there was economic value to a person's control over personal information and "loss of control" was therefore sufficient to attract damages.[21] In addition to appealing to the "intrinsic value" of privacy, claimants in unauthorized use of personal data matters may also seek compensation for intangible harms, such as distress and anxiety without the need to first prove financial loss, as in *Morrisons*.[22]

While claimants may argue that privacy has intrinsic value in unauthorised access to personal data cases as well, US experience suggests they are also likely to claim compensation for more tangible harm. Such claims may include compensation for identity theft monitoring and prevention costs, time spent and/or loss of productivity to address the breach, future risk of identity theft, diminished value of private data, overpayment for service, and loss of access to account funds or adverse credit effects.[23]

Valuing personal data and potential harm due to loss or breach of privacy

The range for the quantum of damages awarded by the Court in past UK data-related cases varies at least from £10 to £18,000 per claimant.[24] Damages estimates will necessarily vary significantly across cases when the facts of the case determine the quantum.

In this section, after a brief description of the types of methodologies that scholars have considered when seeking to value personal data, we discuss the challenges in attaching a monetary value to personal data and privacy.

Methodologies for valuing personal data and potential harm due to loss or breach of privacy

Marketing and economics scholars have considered several methodologies for quantifying the value of personal data and any harm resulting from a loss or breach of privacy. These methodologies, also used for example in competition investigations, fall under two broad categories:

• **Stated Preference Methods** such as contingent valuation and conjoint analysis ask survey respondents questions in a manner that allows the investigator to learn about their preferences about data privacy and/or data breaches. To provide reliable results using these methods requires the expert to take great care when designing, implementing, and interpreting the survey. Done poorly, stated preference methods can produce unreasonably large damages estimates.

• **Revealed Preference Methods** such as natural experiments, event studies, and difference-in-differences analyses rely on real-world data that measures actual behaviour following a "data event" rather than consumers' stated responses. For example, it may be possible to measure changes in private browser usage before and after the news about an infringement was made public. Alternatively, one could assess whether affected individuals took the time and effort to delete the information on their user profiles after the disclosure. If they did not, then it may indicate that they place little value on the data breach at issue. While revealed preference methods can have advantages over stated preference methods, they can also be susceptible to modelling choices, causality issues, and confounding factors, and do rely on assumptions. Applying these methods in a litigation context therefore requires careful thought.

Once any harm resulting from a loss or breach of privacy has been estimated, it is also important to account for relevant benefits that may have accrued to claimants from a company's use of their data. For example, empirical methods could be used to measure whether consumers value online advertising that is targeted to match their preferences. If such targeted advertising provided a positive benefit to the claimant, then the damages calculation – which aims to put the claimant in the position it would have been absent the breach – should reflect the damage from the loss in privacy net of the benefits arising from the breach.

Challenges inherent in attaching value to personal data and privacy

There are several inherent challenges in valuing personal data and any loss of control of personal data. Some of the key issues are discussed below.

The "Privacy Paradox". A central challenge in quantifying the value of privacy is the "Privacy Paradox". Specifically, consumers may behave as if they do not value privacy but, when asked, they may state that they attach a substantial value to it.[25] For instance, consumers typically do not read terms and conditions, and willingly give up a lot personal information when interacting online, yet survey respondents often claim that they attach significant value to at least certain types of personal data.[26]

Heterogeneity in individuals' perceptions of privacy. The literature on privacy finds that the perception of privacy varies considerably across individuals and across contexts.[27] Individuals differ significantly in terms of their expectations regarding whether their information is public or private, and hence their concern for the privacy of their information. For instance, a 2014 survey conducted by UK Information Commissioner's Office showed that 24 per cent of respondents considered their internet browsing history to be "Not sensitive" while the rest considered it "Sensitive" or "Extremely sensitive"[28]. In fact, even a given individual's preference for privacy for the same information can vary by context. [29] Such evidence sits uncomfortably with a notion there is a unique, intrinsic value to privacy or harm due to loss of control of privacy.

The value a firm derives from personal data does not necessarily reflect the damage to claimants from a loss of privacy or personal data. Any value a firm derives from personal data will be affected by numerous factors *other* than the data itself. For example, it may reflect, in part, the value added from data aggregation and processing using the firm's proprietary algorithms. Any approach that relies on the value of the data to the firm would have to separate out the contributions of the other (confounding) factors that influence a firm's valuation, revenues and profits. Moreover, personal data may only be valuable to firms to the extent that it is part of a large dataset. If so, the value of an individual's data may not be easily inferred from the value the firm derives from an aggregation of personal data. Finally, the fact that a firm may benefit from private information does not preclude benefits to users. For example, the information collected may be used to provide better search results and, if so, this benefit must also be quantified and accounted for.

Establishing causality is not always straightforward. Establishing that any loss was directly linked to a specific data breach is important when calculating damages in data breach matters. Given how common data breach incidents are becoming,[30] it may not be straightforward to determine whether a given claimant was impacted by a given data breach (as opposed to a variety of other data breaches that may have affected that same claimant). In addition, there can be other confounding factors—for example, some of the private information may be accessible through means other than the data breach.

Markets where an individual's personal data can be priced legitimately do not ordinarily exist. Evidently, where markets don't exist, there can be no reliable "market price" for an individual's data. While personal data may be available for purchase on the dark web, the price data available from such transactions will reflect a valuation relevant for illicit activities such as identity theft, and may therefore be very different from the value of that data for legitimate activities like targeting online ads. Thus, the price of stolen data on the dark web may not reflect either an individual claimant's valuation or a "minimum" valuation common to all claimants.

Conclusion

The right to compensation in the GDPR and the DPA 2018 have, by design, introduced a significant risk of damages actions following allegations of unauthorised use or access of personal data. The emerging but nascent stage of such litigation in the UK means that experience from other jurisdictions and practice areas can provide significant insight into the likely challenges and opportunities when responding to such damages actions. As in all damages actions, the legal framework, the facts, and the quality of legal ad-

vice and expert evidence will all affect the likelihood of achieving a successful resolution to a dispute.

About the authors

Peter Davis, Louise Freeman, Samid Hussain and Kate Scott.

Peter Davis is a Senior Vice President at Cornerstone Research in London.

Louise Freeman is a Partner at Covington & Burling LLP in London.

Samid Hussain is a Senior Vice President and Head of the Consumer Fraud and Product Liability practice at Cornerstone Research.

Kate Scott is a Partner at Clifford Chance in London.

References

1, Peter Davis is a Senior Vice President at Cornerstone Research in London. Louise Freeman is a Partner at Covington & Burling LLP in London. Samid Hussain is a Senior Vice President and Head of the Consumer Fraud and Product Liability practice at Cornerstone Research. Kate Scott is a Partner at Clifford Chance in London. The views expressed in this article are solely those of the authors, who are responsible for the content, and do not necessarily represent the views of Cornerstone Research, Covington & Burling LLP, or Clifford Chance.

2, Lloyd v Google LLC [2019] EWCA Civ 1599.

3, "YouTube Faces Legal Battle over British Children's Privacy," BBC, 13 September 2020, available at https://www.bbc.com/news/business-54140676, accessed on 21 September 2020.

4, "Hotel group Marriott faces London lawsuit over huge data breach," Financial Times, 19 August 2020, available at https://www.ft.com/content/d6202d00-a173-4b15-b68a-46764934c76b, accessed on 24 September 2020.

5, Various Claimants v WM Morrisons Supermarkets plc (Rev 1) [2017] EWHC 3113 (QB).

6, Weaver & others v British Airways plc, Claim No. BL-2019-001146.

7, Tanya Powley and Kate Beioley "EasyJet Faces Group Legal Claim over Cyber Attack Data Breach," Financial Times, 24 June 2020, available at https://www.ft.com/content/7a1f3add-1882-4ff7-b5ec-e454aa16fd9a, accessed on 14 September 2020.

8, For related discussions of the legal aspects of privacy-related collective actions in the UK, see Lucy Hall, Maxine Mossman, Kate Scott and Haafiz Suleman, "Data Collective Actions: The Costs of Losing Control," Clifford Chance Thought Leadership, 2 April 2020, available at www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/04/data-collective-actions-the-costs-of-losing-control.pdf, accessed on 14 September 2020; and Daniel P. Cooper, Louise Freeman, Rosie Klement, Greg Lascelles, Alexander Leitch and Mark Young, "EasyJet Latest Firm to Face UK Data Breach 'Class Action'," Covington Alert, 8 June 2020, available at www.cov.com/-/media/files/corporate/publications/2020/06/covington-alert-easyjet-latest-firm-to-face-uk-data-breach-class-action.pdf, accessed on 14 September 2020.

9, Lucy Hall, Maxine Mossman, Kate Scott and Haafiz Suleman, op. cit. at endnote 8.

10, GDPR Recital, 5(1)(b).

11, GDPR Recital, 5(1)(a).

12, GDPR, Article 5(1)(e).

13, GDPR Recital, 5(1)(f).

14, DPA 2018, Section 168.

15, GDRP Recital 82.

16, GDRP Recital 85

17, See Lucy Hall, Maxine Mossman, Kate Scott and Haafiz Suleman, op. cit. at endnote 8; and Daniel P. Cooper, Louise Freeman, Rosie Klement, Greg Lascelles, Alexander Leitch and Mark Young, op. cit. at endnote 8.

18, In Lloyd v Google, it is alleged that between April 2011 and February 2012, Google harvested "Browser Generated Information" of approximately 4 million iPhone users without their knowledge or consent, bypassing Safari's privacy settings. Richard Lloyd v. Google LLC [2019] EWCA Civ 1599, ¶ 1. See Louise Freeman, Daniel Cooper, Mark Young, Gregory Lascelles, Fredericka Argent and Rose Klement, "Landmark Case Opens the Door to UK Data Protection Consumer Class Actions," Covington Alert, 10 October 2019, available at https://www.cov.com/-/media/files/corporate/publications/2019/10/landmark_case_opens_the_door_to_uk_data_protection_consumer_class_actions.pdf, accessed on 21 September 2020.

19, For a related discussion, see "Collective Redress Directive—Implications for Data Protection Law," LexisNexis, 21 July 2020, available at https://www.cov.com/-/media/files/corporate/publications/2020/07/collective-redress-directiveimplications-for-data-protection-law.pdf, accessed on 14 September 2020.

20, See, e.g., Opperman v. Path, Case No. 13-cv-00453-JST.

21, Lloyd v Google LLC [2019] EWCA Civ 159, ¶¶ 46, 47.

22, WM Morrisons Supermarkets plc v. Various Claimants [2020] UKSC 12, ¶ 9. This builds on the earlier decision in Google Inc v Vidal-Hall and others [2015] EWCA Civ 311.

23, See, e.g., In re Barnes & Noble Pin Pad Litigation, Case No. 1:12-cv-08617; In re: Brinker Data Incident Litigation, Case No. 18-cv-00686-TJC-MCR; Antman et al. v Uber Technologies, Inc., Case No. 3:15-01175-LB.

24, Examples include TLT v Secretary of State for the Home Office (£2,500 to £12,500); Woolley v Nahid Akbar (£10 per claimant per day); Lloyd v Google (claim for £750 per claimant); easyJet (claim for up to £2,000 per claimant); and Aven and others v Orbis Business Intelligence Ltd (£18,000 per claimant). See also Louise Freeman, Daniel Cooper, Gregory Lascelles, Mark Young, Katharine Kinchlea and Tom Cusworth, "English High Court Awards Damages for Quasi-Defamation Data Claim," Inside Privacy, Covington Alert, 174 September 2020, available at https://www.cov.com/-/media/files/corporate/publications/2020/09/english-high-court-awards-damages-for-quasi-defamation-data-claim.pdf, accessed on 21 September 2020.

25, Sarah Spiekermann, Jens Grossklags and Bettina Berendt (2001), "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior," Third ACM Conference on Electronic Commerce, Tampa, pp. 38–47; Patricia Norberg, Daniel Horne and David Horne (2007), "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," Journal of Consumer Affairs, 41(1), pp. 100–126; Idris Adjerid, Eyal Peer, and Alessandro Acquisti (2018), "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," MIS Quarterly, 42(2), pp. 465–488; Alessandro Acquisti, Laura Brandimarte, and George Loewenstein (2015), "Privacy and Human Behavior in the Age of Information," Science, 347(6221), pp. 509–514 at p. 510.

26, Survey evidence is also sometimes criticised for "focalism bias" which can arise if privacy is not a product "feature" that is typically considered by consumers. See,

e.g., Daniel Kahneman, Alan Krueger, David Schkade, Norbert Schwarz, and Arthur Stone (2006), "Would You Be Happier if You Were Richer? A Focusing Illusion," Science, 312(5782), pp. 1908–1910. For a related criticism of contingent valuation methods, see Jerry Hausman (2012), "Contingent Valuation: From Dubious to Hopeless," Journal of Economic Perspectives, 26(4), pp. 43–56.

27, See, e.g., H. Jeff Smith, Sandra Milberg and Sandra Burke (1996), "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," MIS Quarterly, 20(2), pp. 167–196; Alessandro Acquisti, Laura Brandimarte and George Loewenstein (2015), "Privacy and Human Behavior in the Age of Information," Science, 347(6221), pp. 509–514; Kristen Martin and Katie Shilton (2016), "Why Experience Matters to Privacy: How Context-Based Experience Moderates Consumer Privacy Expectations for Mobile Applications," Journal of the Association for Information Science and Technology, 67(8), pp. 1871–1882.

28, "Annual Track 2014: Individuals (Topline Findings)," Information Commissioner's Office, September 2014, p. 13, available at https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf, accessed on 21 September 2020.

29, See, e.g., Leysia Palen and Paul Dourish (2003), "Unpacking 'Privacy' for a Networked World," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 129–136; Leslie John, Alessandro Acquisti and George Loewenstein (2011), "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," Journal of Consumer Research, 37(5), pp. 858–873; Alessandro Acquisti, Leslie John and George Loewenstein (2012), "The Impact of Relative Standards on the Propensity to Disclose," Journal of Marketing Research, 49(2), pp. 160–174.

30, For example, between 71 per cent (Belgium) and 55 per cent (UK) of European firms reported experiencing cyber attacks in 2019. See "Hiscox Cyber Readiness Report 2019," Hiscox, p. 4, available at www.hiscox.co.uk/sites/uk/files/documents/ 2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF, accessed on 21 September 2020.