Estimating Harm in Invasion of Privacy and Data Breach Disputes


Vildan Altuglu


Vikram Kumar


Vivek Mani


Sinan Corus

Cornerstone Research

1 Introduction

Recent litigation trends in the UK and the US indicate two clear categories of data claim: invasion of privacy cases; and data breach cases. In the case of an invasion of privacy, a consumer's personal data are allegedly misused by the provider of a service or product that collects the data. In the case of a data breach, personal data are compromised as a result of unauthorised third parties accessing the data.

This chapter provides a general overview of the recent developments in the UK and the US in invasion of privacy and data breach cases, and discusses methodologies that frequently have been used by the plaintiffs to estimate damages.

2 Data Privacy and Data Breach Litigation: State of Play in the UK and the US

2.1 The UK

The common features of the recent invasion of privacy private actions in the UK are that they: (i) targeted businesses, such as digital platforms, which offer products that collect or use personal data; and (ii) were filed under the UK's representative action regime, under which a single claimant may sue on behalf of other individuals who share the "same interest" in the litigation, and which may be used to create an opt-out class action.[1]

The most significant invasion of privacy case the UK has seen so far is *Lloyd v. Google*. The dispute relates to Google's placing of "tracking cookies on the Apple Safari browser, allowing it to gather and monetise iPhone users' data" without the users' consent.[2] An opt-out representative action was filed against Google in 2017. The UK High Court dismissed the case in 2018, ruling that the case could not be brought as an opt-out class action through the representative action mechanism, but the judgment was reversed by the UK Court of Appeal a year later.[3] Following the hearing in April 2021, the UK Supreme Court is yet to issue its decision, which is anticipated to be a "watershed moment" for privacy and data protection litigation.[4]

Additional examples of invasion of privacy representative actions in the UK include *Rumbul v. Oracle*, where plaintiffs alleged that Oracle and Salesforce collected personal data of online users and auctioned the data off to third parties without proper consent from the users.[5] In *Elisabeth v. Experian Limited*, Experian PLC, a credit reference agency, was alleged to build profiles of consumers as part of its direct marketing services and sell these data to third parties (such as commercial organisations, charities and political parties) without individuals' knowledge.[6] Similarly, in *Carpio v. Facebook*, plaintiffs alleged that Facebook allowed third parties such as Cambridge Analytica to access and process Facebook users' personal information without their consent or knowledge.[7,8]

In data breach cases, group litigation orders, which require claimants to identify themselves and sign up for the litigation before the judgment stage, were more common.[9] These lawsuits involved a variety of businesses that were alleged to have exposed a wide spectrum of personal data. Recent examples include: litigation against British Airways as a result of a cyber-attack allegedly exposing personal and financial data, including names, addresses and payment-card details of more than 400,000 customers;[10] litigation against EasyJet for allegedly exposing the email addresses and travel details of nine million customers;[11] and litigation against Virgin Media for allegedly exposing names, email addresses, phone numbers and other personal information of one million customers.[12]

2.2 The US

Similar to the UK, recent invasion of privacy cases in the US have involved businesses with access to personal data. For example, in *Brown v. Google*, plaintiffs alleged that Google tracked and collected web browsing data of its users, even under the private browsing mode that should have prevented the tracking of browser information.[13] In *Facebook Inc. Consumer Privacy User Profile Litigation*, plaintiffs claimed that Facebook had harvested and sold user content and information (such as non-public facts about Facebook users or their activities) to third parties, without prior consent. According to plaintiffs, this allowed third parties to engage in psychographic marketing by allowing them to "personally and psychologically target Facebook users" more precisely.[14] In *Vizio Inc. Consumer Privacy Litigation*, plaintiffs alleged that Vizio collected data on viewing habits, use of online services, and other personal data such as IP addresses and zip codes, and shared this information with third parties without "adequately" disclosing it to users.[15]

Recently, there have been several significant data breach cases in the US. For example, in *Marriott International Inc. Data Breach Litigation*, plaintiffs alleged that hackers stole the personal and financial information of over 500 million guests. The allegedly exposed information included names, mailing addresses, phone numbers, email addresses, birth dates, passport numbers and payment-card information.[16] In *Yahoo! Inc. Customer Data Security Breach Litigation*, plaintiffs claimed that between 2012 and 2014, the personal information of more than three billion Yahoo! email account holders were exposed in a series of data breaches. This included private information contained in users' emails, calendars and contacts.[17] Settlement information is publicly available for some data breach consumer class actions in the US. Table 1 provides class size and settlement amount information for a selected group of high-profile consumer class actions in the US over the last three years.

Table 1
High-Profile Data Breach Consumer Class Action Settlements in the US
2018–2021

	Class Action	Settlement Value[1]	Class Size	Settlement Value Per Class Member
1	Equifax Inc. Customer Data Security Breach Litigation	$380,500,000	147,000,000	$2.59
2	Yahoo! Inc. Customer Data Security Breach Litigation	$117,500,000	194,000,000	$0.61
3	Anthem Inc. Data Breach Litigation	$115,000,000	79,150,325	$1.45
4	Premera Blue Cross Customer Data Security Breach Litigation	$32,000,000	8,855,764	$3.61
5	Experian Data Breach Litigation[2]	$22,000,000	14,931,074	$1.47
6	Banner Health Data Breach Litigation	$8,930,000	2,900,000	$3.08
7	21st Century Oncology Customer Data Security Breach Litigation[3]	$7,850,000	2,157,016	$3.64
8	Sonic Corp. Customer Data Security Breach	$4,325,000	1,500,000	$2.88
9	Community Health Systems Inc.	$4,000,000	6,081,189	$0.66
10	Medical Informatics Engineering Inc. Customer Data Security Breach Litigation[4]	$3,750,000	3,900,000	$0.96
11	Morrow et al. v. Quest Diagnostics Inc.	$195,000	34,000	$5.74

Sources

- Law360; Lex Machina; Yahoo Docket Nos. 366-1, 369-2, 414, 497; Yahoo Settlement Notice; Equifax Docket Nos. 374, 956, 1029; Equifax Breach Notice; Equifax Settlement Notice; Anthem Docket Nos. 714-3, 869-8, 916-3, 1046, 1049; Anthem Settlement Notice; Home Depot Docket Nos. 93, 181, 181-2, 260, 261; Home Depot Settlement Notice; Premera Docket Nos. 44, 273-1, 281, 311, 312, 313; Premera Breach Notice; Premera Settlement Notice; Experian Docket Nos. 151, 285, 322, 329; Experian Breach Notice; Experian Settlement Notice; Banner Docket Nos. 115, 182, 198; 21st Century Oncology Docket Nos. 191, 242, 253, 256, 269; 21st Century Oncology Breach Notice; 21st Century Oncology Settlement Notice; Sonic Docket Nos.114, 174; Sony Docket Nos. 128, 190-2, 193, 211; CHS Docket Nos. 54-1, 196, 198-1, 202, 212, 221; MIE Docket Nos. 65, 175-1, 188, 192; MIE Settlement Notice; and Morrow Docket Nos. 1-1, 116, 126.

Notes

[1] Settlement value is inclusive of all relief to class members and other items such as service payments, attorneys' fees, and settlement administration costs. It does not include the value of mandated changes to business practices. Settlement value reports the minimal possible settlement value in cases where the value of the settlement is subject to change or conditional on future developments in the case. Figures are rounded to the nearest dollar.

[2] Settlement value reports the value of the non-reversionary settlement fund, which represents the minimum settlement value. Total settlement value depends on the number of claims filed. According to the Order Regarding Motion for Final Approval, the settlement value was estimated to increase by about $138.8 million, which makes the total settlement value approximately equal to $160.8 million, or an average of approximately $10.77 per class member.

[3] Settlement value reports the value of the non-reversionary settlement fund, which represents the minimum settlement value. Total settlement value depends on the number of claims filed. According to Plaintiffs' Motion for Final Approval, the settlement is valued in excess of $10.9 million, which is an average of approximately $5.05 per class member.

[4] Payments for settlement administration costs and service awards were not paid out of the settlement fund.

As shown in Table 1, settlement values varied substantially and ranged from $381 million (*Equifax Inc. Customer Data Security Breach Litigation*) to $195,000 (*Morrow v. Quest Diagnostics Inc.*). Settlement value per class member also varied substantially, ranging from $5.74 (*Morrow v. Quest Diagnostics Inc.*) to $0.61 (*Yahoo! Inc. Customer Data Security Breach Litigation*).

3 Estimating Harm in Invasion of Privacy and Data Breach Cases

Claimants in the UK sometimes argue that every class member should receive uniform compensation because there is an "intrinsic value" of privacy that is applicable to all affected individuals. For example, in *Lloyd v. Google*, claimants argued that each class member suffered a uniform harm due to losing control of his or her personal data.[18] According to the Information Commissioner, the intervener in the case, the "right to control one's personal data is of intrinsic value", and loss of control should be acknowledged as a form of damage.[19] Data privacy cases in the US have also seen arguments on the basis of an intrinsic value of privacy. For example, in *Brown v. Google*, plaintiffs claimed damages partly because Google's tracking of web browsing activity without users' consent "intruded upon the Plaintiffs' solitude or seclusion" in a manner that was "highly offensive to a reasonable person".[20]

However, assessing damages based on the intrinsic value of privacy presents challenges from an economic perspective. The "value of privacy" has been shown to vary substantially across individuals and across contexts.[21] For instance, Smith, Milberg and Burke (1996) find that those who have been exposed to or been the victim of misuses of their personal information, those who have high levels of cynical distrust or paranoia, or those who reject societal values and norms, tend to hold

stronger concerns regarding information privacy.[22] Acquisti, Brandimarte and Loewenstein (2015) find that contextual cues, such as the cultural environment, physical setting or behaviour of others, can shape an individual's attitude towards privacy. The authors further find that individuals are likely to be uncertain about their own preferences regarding privacy.[23]

An additional challenge for assessing damages in cases involving personal data is the so-called "privacy paradox". Research has found that although consumers frequently voice concern about protecting their privacy, they willingly reveal personal information in the actual marketplace.[24] This disparity between consumers' attitudes toward privacy and actual behaviour naturally complicates any attempt at estimating an intrinsic value of data privacy.

Further, when assessing damages, one needs to account for any benefit consumers may gain from incremental data sharing, which requires a more careful assessment of the costs and benefits in these cases. For example, increased access to personal data may reduce the search costs for consumers, making it easier to identify relevant information and allowing consumers to make optimal purchasing decisions. Goldfarb and Tucker (2011) find that increased access to personal data may allow better ad targeting, allowing consumers to review more relevant content.[25] According to Evans (2009), increased access to personal data may also lower the transaction costs between merchants and consumers, the benefits of which may be passed on to consumers.[26] Further, increased access to personal data may foster innovation. For example, according to Miller and Tucker (2017), data sharing between medical care providers can allow patients to access personalised medical solutions.[27]

Claimants also commonly argue that it is possible to estimate the market value of the data. For example, in *Lloyd v. Google*, the claimants argued that an alternative calculation to uniform damages would be "negotiating" damages, which would be based on "what Google would have paid the users for use of their data for advertising purposes".[28] Similarly, in the *Facebook Inc. Consumer Privacy User Profile Litigation* in the US, plaintiffs claimed that a market for personal information exists and that a market value for the data can be expressed in dollar terms.[29] In *Yahoo! Inc. Customer Data Security Breach Litigation*, plaintiffs argued that the "Dark Web", where malicious actors are able to exchange and monetise compromised personal data, provided a marketplace for the breached data. Plaintiffs considered using "Dark Web" transactions for types of data that were similar to the breached data to assess damages.[30]

However, the legal market for personal data does not exist for many types of data (e.g., social security numbers). In individual instances where there has been some valuation of certain types of data (e.g., web browsing activity on a device[31]), these valuations are likely to be context-dependent and difficult to generalise by reference to other settings. Further, the "Dark Web" does not constitute a legal market or a marketplace that individual consumers would use to monetise their data. The data that are exchanged in these so-called markets are unlikely to be comparable to the data that were breached.[32] It is also not possible to observe the actual transaction prices in these settings, but rather the prices at which the data were offered to potential buyers.[33]

In addition, survey methods have been proposed to assess the value of data in data privacy and data breach cases. For example, in *Haddad v. Bank of Hope*, a consumer class action involving an alleged data breach incident of a bank in the US, the plaintiffs proposed conducting a survey to assess the "economic value" to consumers of protecting personally identifiable data.[34] Similarly, in *Anthem Inc. Data Breach Litigation*, plaintiffs claimed that the defendants did not deliver the data security that was promised on their health insurance products. The plaintiffs proposed conducting conjoint analysis (or a conjoint survey) to estimate the "customer demand for data security". The estimated consumer demand would be used to "simulate" a price indicating what consumers would have paid for the product if the product was initially promised as delivered; that is, with low data security. Plaintiffs proposed calculating a price premium associated with the alleged misconduct as the difference between the actual price that was paid by consumers and the "simulated" price.[35]

Conjoint analysis was developed based on the premise that a product is the sum of its individual attributes, and attempts to estimate consumers' valuation (or willingness to pay) for a specific attribute based on consumers' preferences for the product.[36] There are several challenges to using conjoint analysis to assess the value of personal data.

Conjoint analysis and surveys in general are susceptible to various well-known biases, some of which may be heightened in the context of data privacy. In addition to the "privacy paradox" discussed above, conjoint surveys are susceptible to "focalism bias", or the tendency of survey respondents to "give more weight" to "easily observed and distinctive differences" than they would in real life.[37] As such, the selection of product attributes included in the conjoint survey can have a large impact on the findings. Similarly, conjoint studies that do not accurately mimic consumer decision-making in the real world have been found to generate biased results.[38]

In data breach cases, plaintiffs also pursued compensation associated with the value of time they spent "mitigating increased risk of identity theft" following the breach, as well as compensation for credit monitoring services they required to identify future fraud.[39] However, academic research identified substantial variation in consumers' reactions to a data breach. For example, according to a RAND Corporation survey, after being notified of a data breach: (i) 22% of respondents took no action, which would imply no time lost for these consumers; (ii) 51% of respondents reacted by "changing [their] password or PIN", which would imply non-zero but insignificant time lost; and (iii) only 24% "closed or switched [their] bank account", which would imply significant time lost.[40]

Similarly, there may be substantial variations among class members in terms of credit monitoring costs (including those members of the class who would not sign up for credit monitoring after being informed of the data breach incident). For example, in the US, breached institutions typically have offered free credit monitoring services for a specified period to individuals impacted by the breach incident. An assessment can be made to determine the extent to which the putative class members make use of these free services.

Based on the data, arguments can be made that at least some individuals (e.g., those who do not avail themselves of the free credit monitoring services) would be unlikely to sign up and pay for credit monitoring after being informed of the data breach incident.[41] Further, to the extent plaintiffs actually purchase a credit monitoring service, the prices paid can vary based on the features of the service.[42]

Endnotes

1. "Special Report", *Global Data Review*, June 2021 ("GDR Report"), p. 6.
2. GDR Report, p. 13; "UK – Lloyd v Google: A One-off or the Floodgates Opening for Privacy Class Actions?", Linklaters, October 2019, https://www.linklaters.com/en/insights/blogs/digilinks/2019/october/uk-lloyds-v-google.
3. GDR Report, p. 14.
4. GDR Report, pp. 13–14. In 2012, Google and the US Federal Trade Commission (FTC) reached a settlement in the US for an investigation involving similar claims. As part of that settlement, Google agreed to pay $22.5 million. *See* "Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser", US Federal Trade Commission, August 2012, https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.
5. "Oracle and Salesforce Hit with $10 Billion GDPR Class-Action Lawsuit", *Forbes.com*, August 14, 2020, https://www.forbes.com/sites/carlypage/2020/08/14/oracle-and-salesforce-hit-with-10-billion-gdpr-class-action-lawsuit/?sh=7a9baee6323c; "Internet Users in Line for £500 per Person Damages from Oracle and Salesforce after Class Action Filed at High Court of England and Wales", *The Privacy Collective*, November 2, 2020, https://theprivacycollective.eu/en/privacy-matters/internet-users-in-line-for-500-per-person-damages-from-oracle-and-salesforce-after-class-action-filed-at-high-court-of-england-and-wales.
6. "ICO Takes Enforcement Action against Experian after Data Broking Investigation", Information Commissioner's Office (ICO), October 27, 2020, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation; "Experian Litigation", Harcus Parker, https://harcusparker.co.uk/campaigns/experian-litigation.
7. "Facebook Sued over Cambridge Analytica Data Scandal", *BBC*, October 28, 2020, https://www.bbc.co.uk/news/technology-54722362; "Facebook to Face UK Group Action over Cambridge Analytica Data Use", MLex, October 2020. In February 2021, another similar class action was filed against Facebook Inc. by Peter Jukes, alleging that the company had allowed third parties to harvest user data without their consent. *See* "Facebook Faces New UK Class Action after Data Harvesting Scandal", *Reuters.com*, February 9, 2021, https://www.reuters.com/business/facebook-faces-new-uk-class-action-after-data-harvesting-scandal-2021-02-09. Similarly, another social media platform, TikTok, faces a class action alleging that the platform collects children's personal information, such as their phone numbers, exact location, and biometric data, without the consent or knowledge of the children or their parents. *See* "TikTok Sued for Billions over Use of Children's Data", *BBC*, April 21, 2021, https://www.bbc.co.uk/news/technology-56815480.
8. Relatedly, in 2018, following an investigation on this matter, the Information Commissioner's Office found that Facebook did not adequately monitor the third parties that accessed personal data, which allowed third parties to "harvest" users' data. *See* "ICO Issues Maximum £500,000 Fine to Facebook for Failing to Protect Users' Personal Information", Information Commissioner's Office (ICO), October 2018, https://ico.org.uk/facebook-fine-20181025.
9. GDR Report, p. 6.
10. Claimants and British Airways reached a settlement, but the settlement amount remains confidential. *See* "BA Faces Largest-Ever Group Privacy Claim in UK over Data Breach", *Financial Times*, January 12, 2021, https://www.ft.com/content/f3dc6c8e-0f65-40d0-a5d5-9d57d3f9d0e0; "British Airways Data-Breach Compensation Claim Settled", *BBC*, July 2021, https://www.bbc.co.uk/news/technology-57734946.
11. "EasyJet Faces Group Legal Claim over Cyber Attack Data Breach", *Financial Times*, June 24, 2020, https://www.ft.com/content/7a1f3add-1882-4ff7-b5ec-e454aa16fd9a.
12. "Virgin Media Breach Exposes Data for 900,000 Customers", *Financial Times*, March 5, 2020, https://www.ft.com/content/179182f0-5f0c-11ea-8033-fa40a0d65a98; "You May Be Owed £5,000 from Virgin Media: Thousands Could Get a Payout, Will You?", *Express.co.uk*, https://www.express.co.uk/life-style/science-technology/1348325/Virgin-Media-thousands-could-get-payout-5000-will-you.
13. Complaint and Demand for Jury Trial, *Brown et al. v. Google LLC and Alphabet Inc.*, Case No. 20-3664 (N.D. Cal. June 2, 2020), ¶¶ 1–8.
14. For example, one of such third parties, Cambridge Analytica, was allegedly targeting voters with "content tailored to their predicted psychological proclivities". *See* Second Amended Consolidated Complaint, *In Re: Facebook Inc. Consumer Privacy User Profile Litigation*, Case No. 18-md-02843-VC (N.D. Cal. Aug. 4, 2020), pp. 1–5, 12.
15. Plaintiffs acknowledged that Vizio users can turn off this feature, but claimed that Vizio's disclosures on this issue were insufficient as they were in "obscure sections of its website", only some iterations of privacy policies, and quickly disappearing pop-ups. *See* Second Consolidated Complaint, *In Re: Vizio Inc. Consumer Privacy Litigation*, Case No. 8:16-ml-02693-JLS (C.D. Cal. Mar. 23, 2017), ¶¶ 6–8, 11, 13.
16. First Amended Complaint, *In Re: Marriott International Inc. Data Breach Litigation*, Case No. 8:19-cv-0654 (D. Md. June 20, 2019), ¶¶ 1, 21.
17. Plaintiffs also alleged that Yahoo! did not notify users of the breaches in a timely manner, with the largest of these breaches being fully disclosed more than four years after the fact. *See* Second Amended Consolidated Class Action Complaint, *In Re: Yahoo! Inc. Customer Data Security Breach Litigation*, Case No. 16-md-02752-LHK (N.D. Cal. Apr. 8, 2019), ¶¶ 2–15.
18. GDR Report, pp. 13–18.
19. Intervention by the Information Commissioner in *Lloyd v. Google*, UKSC 2019/0213, ¶¶ 19, 26.
20. According to the plaintiffs, most Americans considered it important or very important to be in control of their own information. *See* Complaint and Demand for Jury Trial, *Brown et al. v. Google LLC and Alphabet Inc.*, Case No. 20-3664 (N.D. Cal. June 2, 2020), ¶¶ 145–154.
21. In *Lloyd v. Google,* Google's counsel challenged the uniform damages approach proposed by the claimant, arguing that there was substantial variation within the class in exposure to the misconduct and to updated privacy policy regulations, and that if calculated, individual damages might not pass the triviality threshold, as required by an earlier ruling of the Court of Appeal. *See* GDR Report, pp. 13–18.
22. H. J. Smith, S. J. Milberg, and S. J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices", *MIS Quarterly* 20, no. 2 (1996), pp. 167–196 at 186.

23. A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and Human Behaviour in the Age of Information", *Science* 347, no. 6221 (2015), pp. 509–514 at 509–512. Findings reported by Schkade and Kahneman (1998) also suggest that individuals may be unable to accurately judge the impact of a potential misuse of their personal data on their life satisfaction. *See* D. A. Schkade and D. Kahneman, "Does Living in California Make People Happy? A Focusing Illusion in Judgments of Life Satisfaction", *Psychological Science* 9, no. 5 (1998), pp. 340–346 at 345.
24. P. A. Norberg, D. R. Horne, and D. A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", *Journal of Consumer Affairs* 41, no. 1 (2007), pp. 100–126.
25. A. Goldfarb and C. E. Tucker, "Privacy Regulation and Online Advertising", *Management Science* 57, no. 1 (2011), pp. 57–71 at p. 57.
26. D. S. Evans, "The Online Advertising Industry: Economics, Evolution, and Privacy", *Journal of Economic Perspectives* 23, no. 3 (2009), pp. 37–60 at pp. 42, 57.
27. A. R. Miller and C. Tucker, "Frontiers of Health Policy: Digital Data and Personalized Medicine", *Innovation Policy and the Economy* 17 (2017), pp. 49–74 at pp. 65–66.
28. GDR Report, p. 20.
29. Second Amended Consolidated Complaint, *In Re: Facebook Inc. Consumer Privacy User Profile Litigation*, Case No. 18-md-02843-VC (N.D. Cal. Aug. 4, 2020), p. 249. Plaintiffs also claimed that: "Facebook's CEO knew that it was worth at least $0.10 for each App to view a user's profile"; "One study … found that an individual's online identity, including hacked financial accounts, can be sold for $1200 on the dark web"; and "Facebook logins can be sold for approximately $5.20 each". *See* Second Amended Consolidated Complaint, *In Re: Facebook Inc. Consumer Privacy User Profile Litigation*, Case No. 18-md-02843-VC (N.D. Cal. Aug. 4, 2020), pp. 249, 289.
30. Declaration of Ian Ratner, CA, CBV, CPA/ABV, ASA, CFE, *In Re: Yahoo! Inc. Customer Data Security Breach Litigation*, Case No. 16-md-02752-LHK (N.D. Cal. July 14, 2018), ¶¶ 11–21, 24–28.
31. *See, e.g.*, the SavvyConnect app, https://www.surveysavvy.com/savvyconnect.
32. In *Yahoo! Inc. Customer Data Security Breach Litigation*, plaintiffs considered using the "Dark Web" prices for email login information and social media login information to determine the value of the breached personal data of Yahoo! account holders. According to the plaintiff, the "Dark Web" price of login details for a Yahoo! or Gmail account was around $1. *See* Declaration of Ian Ratner, CA, CBV, CPA/ABV, ASA, CFE, *In Re: Yahoo! Inc. Customer Data Security Breach Litigation*, Case No. 16-md-02752-LHK (N.D. Cal. July 14, 2018), ¶¶ 21, 24–28, and Table 2.
33. V. Altuglu *et al.*, "Valuation of Privacy: Assessing Potential Harm from Unauthorized Access and Misuse of Private Information in Consumer Class Actions", forthcoming, *Legal Applications of Marketing Theory*, edited by J. Gersen and J. Steckel, p. 11.
34. Expert Report of Jon A. Krosnick, in *Haddad v. Bank of Hope*, Case No. 18-STCV02066 (Cal. Super. Ct. Mar. 28, 2021).
35. Expert Report of Peter E. Rossi, *In Re Anthem Inc. Data Breach Litigation*, Case No. 15-md-02617-LHK (N.D. Cal. Dec. 2, 2016), ¶¶ 105–107.
36. For example, for a chocolate bar, sweetness, nuttiness, nutritional value, product packaging and promotional messages are potential different product attributes. In product liability cases, conjoint analysis is typically used to estimate consumers' willingness to pay, associated with the disputed promotional messages.
37. D. A. Schkade and D. Kahneman, "Does Living in California Make People Happy? A Focusing Illusion in Judgments of Life Satisfaction", *Psychological Science* 9, no. 5 (1998), pp. 340–346.
38. V. Altuglu *et al.*, "An Assessment of Analytical Tools in Product Liability Matters – Perspectives from Economics, Marketing, and Consumer Behaviour", *International Comparative Legal Guide to Product Liability 2019*, p. 3.
39. Plaintiffs' Third Amended Consolidated Class Action Complaint, *In Re: Zappos Inc. Customer Data Security Breach Litigation*, Case No. 3:12-cv-00325-RCJ-VPC (D. Nev. Sept. 28, 2015), ¶¶ 7, 66, 209.
40. L. Ablon *et al.*, "Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information", RAND Corporation (2016), Table 2.4; V. Altuglu *et al.*, "Valuation of Privacy: Assessing Potential Harm from Unauthorized Access and Misuse of Private Information in Consumer Class Actions", forthcoming, *Legal Applications of Marketing Theory*, edited by J. Gersen and J. Steckel, p. 16.
41. For example, according to a *New York Times* article, only about 3.3 million individuals (out of 147 million individuals eligible for settlement) signed up for the free credit monitoring services offered by Equifax. *See* "Equifax Breach Affected 147 Million, but Most Sit Out Settlement", *New York Times*, January 22, 2020, https://www.nytimes.com/2020/01/22/business/equifax-breach-settlement.html.
42. *See, e.g.*, "Compare Identity Protection Providers", Identity ProtectionReview.com, https://www.identityprotectionreview.com/comparison?land=2.

Vildan Altuglu is a vice president in Cornerstone Research's New York office. She applies economic analysis and marketing research techniques to matters involving product liability, product misrepresentation, false advertising, antitrust, intellectual property, and general business litigation. She is a leader of the firm's consumer fraud and product liability practice. Dr. Altuglu has experience in cases involving data breaches and allegations of unauthorised access to personally identifying data.

Cornerstone Research
599 Lexington Avenue, 40th Floor
New York, NY 10022-7642
USA

Tel: +1 212 605 5006
Email: valtuglu@cornerstone.com
URL: cornerstone.com

Vikram Kumar is a principal in Cornerstone Research's London office. He analyses economic and statistical issues arising in antitrust and competition, product liability, and life sciences matters. He has developed theoretical and numerical models to analyse large, complex datasets in a variety of contexts, and has designed and implemented large-scale market surveys.

Cornerstone Research
4 More London Riverside, 5th Floor
London SE1 2AU
United Kingdom

Tel: +44 20 3655 0902
Email: vkumar@cornerstone.com
URL: cornerstone.com

Vivek Mani is a principal in Cornerstone Research's Boston and London offices. He has over a decade of experience leading teams and consulting to clients on regulatory and litigation issues involving competition. His expertise includes collective actions, cartels and mergers in Europe and the US. Mr. Mani has analysed relevant markets, competitive effects and damages in numerous competition matters. *Who's Who Legal* has recognised him as a future leader in the competition field.

Cornerstone Research
699 Boylston Street, 5th Floor
Boston, MA 02116-2836
USA

Tel: +1 617 927 3194 /
+44 20 3655 0904
Email: vmani@cornerstone.com
URL: cornerstone.com

Sinan Corus is a manager in Cornerstone Research's London office. He provides economic and financial analysis and expert support in all phases of commercial litigation in the UK, US and Europe. His experience includes: merger review; assessment of economic damages related to disputes involving monopolisation, product liability, alleged corporate disclosure misrepresentations and unfair pricing; and *ex post* assessment of competition policy actions.

Cornerstone Research
4 More London Riverside, 5th Floor
London SE1 2AU
United Kingdom

Tel: +44 20 3655 0912
Email: scorus@cornerstone.com
URL: cornerstone.com