

Assessing Health Data Privacy Damages During A Pandemic

By Vildan Altuglu, Maria Salgado and Omur Celmanbet

(September 8, 2020, 4:53 PM EDT)

The COVID-19 pandemic, which has generated a surge in telehealth and introduced the concept of contact tracing into our daily lives, is likely to expose businesses and governments to an increased risk of data privacy and data breach class actions related to health and other personal data.

This article discusses potential economic approaches and challenges to valuing, in class action settings, alleged unconsented use or misappropriation of health and other private data generated during this health crisis.

Class Actions Related to Health Data Privacy and Data Breaches Are Expected to Rise During COVID-19

The spike in the use of telehealth has been one of the dramatic changes in health care delivery since the beginning of the COVID-19 pandemic. Telehealth includes, among others, the practice of doctors caring for patients remotely through the use of tools such as teleconferencing and videoconferencing.

The ability to receive care without having to travel to health care facilities has increased the appeal of telehealth, including telemedicine visits, for many patients during the pandemic. According to an April study, there is a strong correlation between the U.S. population's interest in telehealth and the number of COVID-19 cases.[1]

Similarly, an analysis published by the Commonwealth Fund shows that the share of physician visits conducted via telehealth was practically nonexistent in the first two months of 2020 and rose to nearly 14% by mid-April, as shown below.[2]



Vildan Altuglu

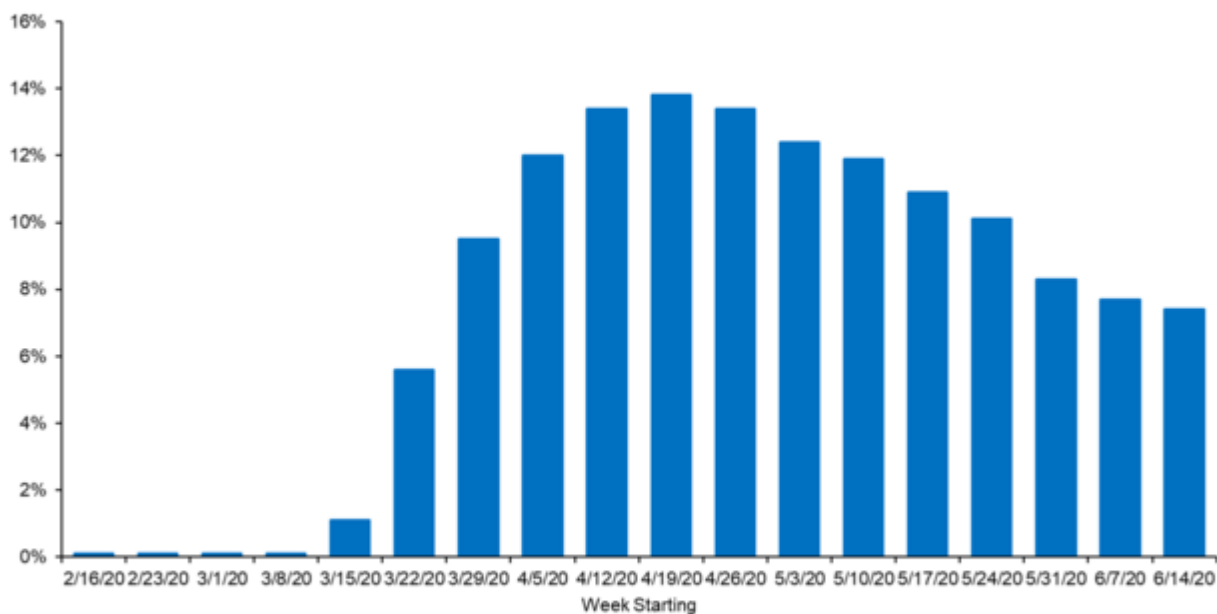


Maria Salgado



Omur Celmanbet

Share of Physician Visits Conducted Via Telemedicine 2/16/20 – 6/14/20



Source: Commonwealth Fund; Phreesia

Note: Data represent percentages; the numerator is the number of telemedicine visits in a given week and the denominator is the number of visits in the baseline week of 3/1/20–3/7/20. Telemedicine includes telephone and video visits.

To facilitate the expansion of telehealth during the pandemic, in March the Office for Civil Rights at the U.S. Department of Health and Human Services lifted certain privacy and security compliance penalties and enforcement actions against providers, allowing them to use audio or video communication technologies, such as Facebook Messenger video chat, Google Hangouts video, Zoom and Skype, to provide remote health care services.[3]

Given the sensitive nature of the data exchanged during telehealth visits and stored by telehealth providers, the use of such communication technologies raises concerns about susceptibility of health and other personal data to unauthorized disclosures, uses, or misappropriation by unauthorized third parties, such as hackers.

These privacy and security concerns also extend to devices patients use to communicate and exchange data with their telehealth providers, including smartphones, tablets and computers as well as in-home patient monitors or other remote-care devices. Unauthorized third parties may obtain personal information, including health data and payment information, or infiltrate the larger networks of patient data in the event they are able to gain access to these connected devices.[4]

Contact tracing is another change facilitated by the pandemic that has led to an increase in exchange of personal data among individuals, companies and governments. Contact tracing is a public health management tool and involves identifying and monitoring individuals who had contact with infected individuals and notifying them of their potential exposure. While there is no compulsory digital COVID-19 contact tracing program in the U.S., multiple voluntary mobile apps developed by private companies exist.[5]

With contact tracing initiatives, the COVID-19 status and geolocation of individuals are collected, stored and also sometimes shared with various entities, raising data privacy and data breach concerns.[6] For example, geolocation data collected from smartphones with contact tracing apps may be used in isolation or in combination with other data to uncover a variety of information about individuals, including their routine activities (e.g., medical intake), interests (e.g., gym membership) and affiliations (e.g., religious affiliation).

Beyond concerns about public disclosure of this personal information, there are also concerns that hackers can create fake contact tracing apps, or send fake messages pretending to be contact tracers to initiate a malware attack or a phishing scam to extract credit card and other personal data.[7]

Accordingly, such changes instituted during the pandemic with regard to health care delivery and public health management are expected to increase class action litigation related to data privacy and data breaches in the health care industry.

Potential Economic Approaches and Challenges to Valuing Alleged Misuse or Misappropriation of Personal Data

Broadly, there are two types of consumer class actions related to personal data: (1) data privacy class actions where the data at issue was allegedly misused by the parties that received the data, and (2) data breach class actions where the data at issue was exposed and improperly accessed by unrelated third parties.

An example of the former is a federal lawsuit filed in 2018 against CVS Health Corp. due to its alleged exposure of the personal health information of over 6,000 individuals via clear-windowed mailings revealing their names, addresses and HIV status.[8] An example of the latter involves lawsuits against Anthem Inc. following a data breach incident that allegedly exposed personal data on 80 million individuals, including names, birth dates, medical identification numbers and social security numbers.[9]

In data privacy class actions, damages pursued are often based on alleged loss of intrinsic value of privacy and alleged unjust enrichment of the party that has misused the data. In data breach class actions, on the other hand, damages pursued are often based on actual fraud costs, future risk of identity theft and identity theft monitoring and prevention costs.[10] The economic approaches related to these theories of harm for telehealth, contact tracing and other personal data are discussed next.

Loss of Intrinsic Value of Privacy

This theory is traditionally built on the premise that keeping information private has a uniform economic value that is common to all individuals (e.g., a societal value), and unauthorized access to this information by a third party would result in the loss of that value.[11] Such a common, uniform value to privacy implies that the alleged injury is not specific to the individual or the infringing party, rendering an identical quantum of damages for each putative class member, regardless of their individual circumstances.

For example, under this theory, unauthorized use of geolocation or health data exchanged as part of COVID-19 contact tracing initiatives would generate the same amount of damages for each putative class member regardless of the extent of information provided by a given individual.

Similarly, unauthorized use of geolocation data accessed by means unrelated to the alleged misconduct

would generate identical damages (e.g., damages due to unauthorized use of geolocation data would be identical whether the data was accessed via a gaming app or via a contact tracing app).

Further, public disclosure of the at-issue information in other contexts (e.g., an infected individual posting COVID-19 status in a public Facebook profile) is unlikely to matter under the loss of intrinsic value of privacy theory.

Survey-based, quantitative approaches such as contingent valuation surveys and conjoint analysis have been proposed as suitable methods to estimate invasion of privacy damages in data privacy class actions.[12] In contingent valuation surveys, respondents are typically asked directly about their value for the conduct at issue.

In the data privacy context, this could include questions such as "how much would you pay to protect privacy of your data?" In conjoint analysis, respondents are typically asked to make choices from a small set of products and services in a series of survey questions.

In the data privacy context, each product or service shown to respondents (e.g., a new online video gaming service) would be described on the basis of the same set of features including a feature that relates to the use or sharing of personal data (e.g., type of game, number of players, whether the service shares players' personal data with advertisers) and a set of prices. Respondents' product choices that involve different feature combinations and prices are then used to estimate an average value for data privacy.

These approaches have been subject to a number of critiques.

First, both contingent valuation and conjoint analysis are stated preference methods in that they rely on what people say or imply they will do (i.e., based on their choices in a survey setting), and not on what they actually do.[13]

Second, in the privacy context, survey methods are subject to the so-called privacy paradox, the well-documented discrepancy between consumers' stated preferences for privacy and their privacy-related behaviors.[14]

Third, both methods have been shown to generate inflated values for privacy due to certain biases these surveys are susceptible to (e.g., conjoint surveys may artificially focus survey respondents on privacy).[15]

Further, reliably extrapolating the estimated average value of privacy beyond the survey samples (e.g., to the putative class as a whole) is challenging due to the extent of heterogeneity in consumers' privacy expectations and preferences.[16]

Unjust Enrichment

An alternative theory of harm put forward in data privacy class actions is based on the allegation that the infringing third party generated revenues and profits by using private data without authorization. Generating reliable estimates of privacy value based on this theory requires distinguishing and isolating the portion of the infringer's valuation, revenues or profits that is directly attributable to the alleged misuse of private data.

This can be a challenging exercise, as numerous factors may influence a firm's valuation, revenues, and profits. For example, determining the value to companies involved in an alleged unauthorized use of geolocation and other private data shared with contact tracing apps would require controlling for all factors that influence these companies' valuation, revenues and profits.

Actual Fraud Costs

In data breach class actions, one of the most commonly pursued type of damages involves actual fraud costs. In the case of breach of payment card data, for instance, this often involves determining fraudulent transactions and associated amounts on exposed accounts. However, because consumers typically share the same types of data with multiple parties and because concurrent data breach incidents have become increasingly common, it can be difficult to establish causality, or a nexus between fraudulent activity and a particular data breach incident.

According to a 2019 industry study, for example, there were 1,473 data breaches in the U.S. in 2019 alone, and over 164 million personally identifiable records were exposed in those breaches.[17] Similarly, a 2016 study showed that roughly 36 million U.S. adults received more than one notification of data breach between June 2014 and June 2015 alone.[18]

Risk of Future Identity Theft

Harm arising from the risk of future identity theft is also commonly pursued in data breach class actions. This theory of harm is based on the premise that the identity theft or other negative consequences of a data breach may not occur immediately. As such, it is argued that individuals whose information was breached should be compensated for the expected long-term impact of the data breach.

Historical evidence and academic literature, however, suggest that only a small number of individuals will experience any type of identity theft as a result of a data breach incident.[19] Moreover, it is difficult to predict who will be impacted: The probability that an individual will be subject to future identity theft can vary across individuals based on prior incidence of identity theft, number of companies that have access to the data at issue, and the type of data that was compromised.

Further, any methods proposed to calculate this type of damages would need to be able to isolate the incremental risk associated with the data breach for each individual in the future.

Identity Theft Monitoring and Prevention Costs

Yet another common type of damages asserted in data breach class actions is based on what consumers allegedly already paid or would likely pay for credit and identity theft monitoring and prevention services. These may include a range of services such as credit freezes with credit reporting agencies, identity theft insurance and credit monitoring services.

Since not everyone would sign up for these types of services, determining which members of a proposed class incurred or would likely incur such costs is central to quantifying these damages. Survey methods soliciting self-reported measures from a sample of putative class members on the costs already incurred and the probability of signing up for credit monitoring or identity theft insurance services may be used. The validity of these methods will in part depend on the reliability of the self-reported measures and on the representativeness of the survey respondents.

Additionally, real-world data may provide insight about the rate at which affected individuals are likely to sign up for credit and identity theft monitoring and prevention services. For example, many companies in the U.S. offer free credit monitoring services to individuals whose data were potentially exposed in a data breach incident. The share of individuals who sign up for these free services, which is typically low, can be informative of the share of individuals who would ultimately sign up and pay a fee for such services.

Vildan Altuglu and Maria Salgado are vice presidents and Omur Celmanbet is a principal at Cornerstone Research.

Cornerstone Research senior manager Rezwan Haque and associate Lucia Yanguas contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the organization, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Young-Rock Hong et al., "Population-Level Interest and Telehealth Capacity of US Hospitals in Response to COVID-19: Cross-Sectional Analysis of Google Search and National Hospital Survey Data," *JMIR Public Health and Surveillance* 6, no. 2 (2020): e18961.

[2] Ateev Mehrotra et al., "The Impact of the COVID-19 Pandemic on Outpatient Visits: A Rebound Emerges," *The Commonwealth Fund*, May 19, 2020.

[3] "Notification of Enforcement Discretion for Telehealth Remote Communications during the COVID-19 Nationwide Public Health Emergency," U.S. Department of Health and Human Services, available at <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html>, last accessed March 27, 2020.

[4] See, e.g., Joseph L. Hall and Deven McGraw, "For Telehealth to Succeed, Privacy and Security Risks Must Be Identified and Addressed," *Health Affairs* 33, no. 2 (2014): 216–221. See also Lily Hay Newman, "Medical Devices Are the Next Security Nightmare," *Wired*, March 2, 2017.

[5] See "Coronavirus Disease 2019 (COVID-19): Contact Tracing," Centers of Disease Control and Prevention, August 4, 2020, available at <https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/contact-tracing.html>.

[6] See Paige M. Boshell, "The Power of Place: Geolocation Tracking and Privacy," *American Bar Association Business Law Section*, March 25, 2019.

[7] See Stephen Silver, "Fake Contact Tracing Apps Could Install Malware on Your Smartphone," *The National Interest*, June 12, 2020. See also Lily Hay Newman, "Don't Be Fooled by Covid-19 Contact-Tracing Scams," *Wired*, May 25, 2020.

[8] Class Action Complaint, *John Doe One et al. v. CVS Health Corp. et al.*, No. 2:18-cv-00238-EAS-CMV (S.D. Ohio, Mar. 21, 2018).

[9] Class Action Complaint, *Brown v. Anthem Inc.*, No. 5:15-md-02617 (N.D. Cal., Feb. 13, 2015).

[10] See Vildan Altuglu, Lorin M. Hitt, S. Hussain, and M. Li Bergolis, "Valuation of Privacy: Assessing Potential Harm from Unauthorized Access and Misuse of Private Information in Consumer Class Actions," forthcoming in *Legal Applications of Marketing Theory*, eds. Professors Jacob Gersen and Joel Steckel.

[11] See Vildan Altuglu, Lorin M. Hitt, S. Hussain, and M. Li Bergolis, "Valuation of Privacy: Assessing Potential Harm from Unauthorized Access and Misuse of Private Information in Consumer Class Actions," forthcoming in *Legal Applications of Marketing Theory*, eds. Professors Jacob Gersen and Joel Steckel.

[12] See Vildan Altuglu, Lorin M. Hitt, S. Hussain, and M. Li Bergolis, "Valuation of Privacy: Assessing Potential Harm from Unauthorized Access and Misuse of Private Information in Consumer Class Actions," forthcoming in *Legal Applications of Marketing Theory*, eds. Professors Jacob Gersen and Joel Steckel.

[13] See, e.g., Jerry Hausman, "Contingent Valuation: From Dubious to Hopeless," *Journal of Economic Perspectives* 26, no. 4 (2012): 43–56.

[14] See, e.g., Sarah Spiekermann, Jens Grossklags, and Bettina Berendt, "E-Privacy in 2nd Generation E-commerce: Privacy Preferences versus Actual Behavior," in *Proceedings of the 3rd ACM Conference on Electronic Commerce* (2001): 38–47; Patricia A. Norberg, Daniel R. Horne, and David A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* 41, no. 1 (2007): 100–126; Idris Adjerid, Eyal Peer, and Alessandro Acquisti, "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," *MIS Quarterly* 42, no. 2 (2018): 465–488; Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science* 347, no. 6221 (2015): 509–514 at 510.

[15] See, e.g., Jerry Hausman, "Contingent Valuation: From Dubious to Hopeless," *Journal of Economic Perspectives* 26, no. 4 (2012): 43–56.

[16] Academic research demonstrates that consumers differ in their privacy preferences and expectations and that consumers' privacy preferences and expectations can be context-dependent. See, e.g., Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science* 347, no. 6221 (2015): 509–514; Kirsten Martin and Katie Shilton, "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, no. 8 (2016): 1871–1882; Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review* 79, no. 1 (2004): 119–157.

[17] "2019 End-Of-Year Data Breach Report," Identity Theft Resource Center, 2020, available at <https://notified.idtheftcenter.org/s/resource>.

[18] Lillian Ablon et al., "Consumer Attitudes toward Data Breach Notifications and Loss of Personal Information," Rand Corporation, 2016. The actual number of data breaches is likely to be higher: a recent study estimated the number of unreported data breaches may be equal to 25 percent to 85 percent of the number of reported breaches. See James T. Graves, Alessandro Acquisti, and Nicolas Christin, "Should Credit Card Issuers Reissue Cards in Response to a Data Breach? Uncertainty and Transparency in Metrics for Data Security Policymaking," *ACM Transactions on Internet Technology*

(TOIT) 18, no. 4 (2018): 1–19.1847, no. 6221 (2015): 509-514.

[19] See, e.g., "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," U.S. Government Accountability Office, GAO-07-737, June 2007.

Estimating Harm in Invasion of Privacy and Data Breach Disputes

Cornerstone Research



Vildan Altuglu



Vikram Kumar



Vivek Mani



Sinan Corus

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	Premiera 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	21 st 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; Premiera Docket Nos. 44, 273-1, 281, 311, 312, 313; Premiera Breach Notice; Premiera 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 device³¹), 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-md-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-RJ-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](https://www.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 data-sets 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](https://www.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](https://www.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](https://www.cornerstone.com)

Cornerstone Research provides economic and financial consulting and expert testimony in all phases of complex disputes and regulatory investigations. The firm works with an extensive network of prominent academics and industry practitioners to identify the best-qualified expert for each assignment. Cornerstone Research has earned a reputation for consistent high quality and effectiveness by delivering rigorous, state-of-the-art analysis for more than 30 years. The firm has over 700 staff and offices in Boston, Chicago, London, Los Angeles, New York, San Francisco, Silicon Valley, and Washington, D.C. To connect with us, please visit <https://www.linkedin.com/company/cornerstone-research>.

www.cornerstone.com

**CORNERSTONE
RESEARCH**



PRIVACY-ENHANCING TECHNOLOGIES IN ADTECH AND CONSUMERS' PERCEIVED PRIVACY VIOLATIONS



**BY
KINSHUK
JERATH**



**&
LORENZO
MICHELOZZI**

Kinshuk Jerath is the Arthur F. Burns Chair of Free and Competitive Enterprise, Professor of Business in the Marketing Division at the Graduate School of Business, Columbia University. Lorenzo Michelozzi is a Principal at Cornerstone Research. The views expressed herein are those of the authors and do not necessarily represent the views of Cornerstone Research. This article is based in part on academic work that Kinshuk Jerath conducted together with Klaus Miller. Klaus Miller is an Assistant Professor in the Marketing Department at HEC Paris and a Chairholder at the Hi!Paris Center on Data Analytics and Artificial Intelligence for Science, Business and Society. The authors thank Coby Wittman for his outstanding assistance with the preparation of this article. Coby Wittman is an Associate at Cornerstone Research.

PRIVACY-ENHANCING TECHNOLOGIES IN ADTECH AND CONSUMERS' PERCEIVED PRIVACY VIOLATIONS

By Kinshuk Jerath & Lorenzo Michelozzi



HEALTH DATA AND THE FUTURE OF ADTECH

By Aaron Burstein, Alysa Hutnik & Meaghan Donahue



WHY ARE THE DOJ AND EU COMMISSION LOOKING TO BREAK UP GOOGLE?

By Tim Cowen



TESTIMONY BEFORE THE U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON THE JUDICIARY HEARING ON "COLLUSION IN THE GLOBAL ALLIANCE FOR RESPONSIBLE MEDIA"

By Spencer Weber Waller



PRIVACY-ENHANCING TECHNOLOGIES IN ADTECH AND CONSUMERS' PERCEIVED PRIVACY VIOLATIONS

By Kinshuk Jerath & Lorenzo Michelozzi

In response to growing consumer privacy concerns and governmental regulations, privacy-enhancing technologies ("PETs") are being developed in the AdTech space to allow ad targeting while limiting the flow and use of user data relative to current practices. Will PETs succeed in alleviating consumers' privacy concerns? A recent study by Professors Kinshuk Jerath and Klaus Miller suggests that PETs can reduce consumers' perceived privacy violations relative to current practices. The reduction, however, is small. Other practices that do not allow the targeting of online ads based on consumer behavior, such as contextual advertising, achieve more substantial reductions. These findings suggest that consumers' perceived privacy violations are affected less by technical details of whether/how the data is shared and more by expectations on how it is used and how individual-specific the outcomes will be. A consumer-centric approach to developing privacy solutions in AdTech, which more holistically considers consumers' perceived privacy violations, is recommended. Consumer education on privacy-enhancing initiatives may also help to bridge the gap between technical definitions of privacy and consumers' perceptions.

Visit www.competitionpolicyinternational.com for access to these articles and more!

Scan to Stay Connected!

Scan here to subscribe to CPI's
FREE daily newsletter.



01

INTRODUCTION

Growing privacy concerns among consumers over the use of their data for online advertising have spurred the development and implementation of *privacy-enhancing technologies* (“PETs”).² PETs are intended to allow advertisers to target relevant audiences online while limiting the flow and use of consumer data that is required to do so. While the technical aspects of PETs have received considerable attention, little is known about how consumers may receive them. Will PETs succeed in alleviating privacy concerns about the collection and use of consumer data for targeted advertising?

A recent study by Professors Kinshuk Jerath and Klaus Miller sheds light on this question. The authors use an online experiment to examine consumers’ perceptions of privacy violations for current advertising practices as well as for practices akin to certain prominent PETs being implemented or developed. These PETs allow firms to target ads to individual users based on data that does not leave consumers’ devices and is therefore not shared with third parties. The authors find that, relative to current practices, these PETs can reduce consumers’ perceived privacy violations. The reduction, however, is small. Other practices that do not target advertising based on consumer characteristics or browsing histories, such as contextual advertising, reduce consumers’ perceived privacy violations more substantially. The experimental results of Jerath and Miller suggest that consumers’ perceived privacy violations are affected less by whether/how the data is shared (does it leave the device?) and more by expectations on how it is used and how individual-specific ads can get (is the data used to target ads effectively based on behavior?).

This article first provides an introduction to PETs and discusses some prominent examples being developed as part of Google’s Privacy Sandbox. It then presents the findings of the Jerath and Miller study and discusses their interpretation. The article concludes by elaborating on the implications of the findings. Firms and policy-makers may want

to adopt a consumer-centric approach to PETs that more holistically considers consumers’ perceived privacy violations and also addresses the tradeoff that consumers face in practice between the perceived privacy costs of sharing data and the benefits that arise from the provision of advertising-funded content and services online. Consumer education on privacy-enhancing initiatives may also help to bridge the gap between technical definitions of privacy and consumers’ perceptions.

02

THE EMERGENCE OF PRIVACY-ENHANCING TECHNOLOGIES IN RESPONSE TO PRIVACY CONCERNS

Behavioral targeting has become the online advertising industry’s standard for display advertising. Under behavioral targeting, information about a consumer’s activity is tracked over time and across websites and used to build user-level profiles attempting to understand the consumer’s demographic characteristics (e.g. gender, age group, location) and interests (e.g. travel, fitness, sport). Consumers’ characteristics and interests can then be used to target the ads that consumers encounter as they consume online content and services. Targeted ads have been shown to be more effective than untargeted ones,³ suggesting that targeting improves the relevance of these ads to consumers. And to this day, online advertising remains the main source of revenue for many websites and publishers, allowing them to offer high-quality and free content and services to consumers.⁴

While targeted ads support online content and services that consumers enjoy, behavioral targeting elicits privacy con-

2 PETs can broadly be defined as technologies that “permit the collection, processing, analysis, and sharing of information, while protecting the confidentiality of personal data.” See *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, OECD Digital Economy Papers (March 8, 2023), <https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm>.

3 See, e.g. Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, *Management Science* 57(1), 57-71 (2011); Paul R. Hoban & Randolph E. Bucklin, *Effects of Internet Display Advertising in the Purchase Funnel: Model-Based Insights from a Randomized Field Experiment*, *Journal of Marketing Research* 52(3), 375-393 (2015); Nils Wernerfelt, Anna Tuchman, Bradley Shapiro & Robert Moakler, *Estimating the Value of Offsite Tracking Data to Advertisers: Evidence from Meta*, forthcoming in *Marketing Science*.

4 Benjamin Shiller, Joel Waldfogel & Johnny Ryan, *The Effect of Ad Blocking on Website Traffic and Quality*, *The RAND Journal of Economics* 49(1), 43-63 (2018).

cerns.⁵ In response to these and other similar concerns, privacy regulation has become more stringent with the introduction of laws, such as the General Data Protection Regulation (“GDPR”) in the European Union or the California Consumer Privacy Act (“CCPA”), which seek to give users more control over their data and require firms to give users the right to opt-out from sharing their personal information. Recognizing consumer apprehension to data sharing, in the last few years, private companies have also launched initiatives to limit data collection and behavioral tracking and give consumers more control over their data. For example, in 2021, Apple adopted App Tracking Transparency, a framework that requires iOS apps to request permission from users before tracking their activity across other companies’ apps or websites or sharing data with data brokers.⁶ Web browsers such as Firefox and Safari have taken measures to stop third parties from tracking users’ activity across websites by disabling third-party cookies as part of their standard settings.⁷

Against this backdrop, firms have also begun implementing or developing PETs to maintain the efficacy of advertising while addressing privacy concerns. Some of the most prominent examples of PETs are being developed under Google’s Privacy Sandbox, an initiative that aims to reduce cross-site tracking while allowing publishers and developers to serve relevant content and ads.⁸ Within the Sandbox toolkit, Google proposed two technologies that would directly impact how behavioral data used to target online ads is collected, processed, and shared: “Topics” and “Protected Audience.”⁹

The “Topics” technology allows web browsers to infer interest-based categories associated with the websites a consumer visits. For example, the browser would match

a sports website with the topic “Sports.” This matching process occurs on the consumer’s device without sharing information about the specific website visited with third parties, as it is currently done, for example, by third-party cookies. The most frequent topics associated with the websites visited by the consumer would then be shared with advertisers to help them show ads relevant to these topics on the websites the consumer visits.¹⁰

“Against this backdrop, firms have also begun implementing or developing PETs to maintain the efficacy of advertising while addressing privacy concerns”

The “Protected Audience” technology uses a consumer’s activity to assign them to audiences that advertisers have defined for ad targeting purposes. For example, a bike maker may have defined an audience of “mountain bike enthusiasts” for consumers that have browsed mountain bikes on its website.¹¹ The “Protected Audience” technology allows the bike maker to show ads about mountain bikes to members of this audience when they visit a different website, say a sports magazine’s site. Unlike current practices, the process that leads to the display of the bike maker’s ad on the sports magazine’s webpage occurs

5 For example, according to a 2019 Pew Research survey, 79 percent of Americans were concerned about how their data is collected and used by companies. This figure rose to 81 percent in a similar survey conducted in 2023. Additionally, according to the 2019 survey, 81 percent of Americans thought the risks of data collection outweigh the benefits. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (November 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>; Colleen McClain et al., *How Americans View Data Privacy*, Pew Research Center (October 18, 2023), <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>.

6 Kinshuk Jerath, *Mobile Advertising and the Impact of Apple’s App Tracking Transparency Policy* (April 26, 2022), https://www.apple.com/privacy/docs/Mobile_Advertising_and_the_Impact_of_Apples_App_Tracking_Transparency_Policy_April_2022.pdf.

7 Marissa Wood, *Today’s Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default*, Firefox (September 3, 2019), <https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/>; Nick Statt, *Apple Updates Safari’s Anti-Tracking Tech with Full Third-Party Cookie Blocking*, The Verge (March 24, 2020), <https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking>; John Wilander, *Full Third-Party Cookie Blocking and More*, WebKit (March 24, 2020), <https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/>.

8 Google, as well, had seriously considered disabling third-party cookies from the Chrome browser. However, it recently decided to keep them as it continues to develop its Privacy Sandbox initiatives. See *Protecting Your Privacy Online*, Google Privacy Sandbox, <https://privacysandbox.com/>; *Prepare for the third-party cookie phaseout*, Google Privacy Sandbox (March 13, 2024), <https://developers.google.com/privacy-sandbox/3pcd/prepare/prepare-for-phaseout>; Anthony Chavez, *A New Path for Privacy Sandbox on the Web*, The Privacy Sandbox (July 22, 2024), <https://privacysandbox.com/news/privacy-sandbox-update/>.

9 *Technology for a more private internet*, Google Privacy Sandbox, <https://privacysandbox.com/learning-hub/>.

10 *Topics*, The Privacy Sandbox, <https://privacysandbox.com/proposals/topics/>.

11 *Protected Audience API overview*, Privacy Sandbox (January 27, 2022), <https://developers.google.com/privacy-sandbox/relevance/protected-audience>.

on the consumer's device.¹² Thus, while “Protected Audience” allows for more fine-grained targeting than “Topics,” a key common feature of both these targeting technologies is that they keep the consumer's information on the consumer's device without sharing their browsing histories with third parties.

While PETs ultimately aim to benefit consumers by improving privacy protections, little is known about consumers' perceptions of PETs' ability to address privacy concerns. In fact, a lot of the discussion about PETs has been devoted to technical aspects and details related to data collection and usage by firms that PETs permit.¹³ However, because digital advertising relies on consumer-facing technologies, it is important to understand whether and how these technologies can successfully address consumers' needs and wants.¹⁴ Understanding consumers' perceptions is also important for policy-makers if their goal is to ensure that privacy regulations adequately address consumers' concerns.

03

NEW EVIDENCE ON CONSUMER PERCEPTIONS OF PRIVACY VIOLATIONS

In order to evaluate privacy violations that consumers may perceive in relation to behavioral tracking and PETs, it is

important to understand the two types of value consumers place on privacy. The first is the intrinsic value of privacy, which refers to the disutility consumers may experience when their information is shared, regardless of how their information is used (even if not used at all). The second is the instrumental value of privacy, which refers to the disutility consumers experience if they dislike how their information is used (e.g. internet browsing information may allow firms to price discriminate, leading certain consumers to be charged higher prices). Instrumental value can also refer to the positive utility that consumers experience if, instead, they like how the information is used (e.g. video-content recommendations based on viewing history). While PETs may work to address the intrinsic value of privacy (e.g. by stopping consumer data from leaving their local device), they may not address the instrumental value if consumers find that companies can effectively use their data for profiling and targeting even if it was processed locally.

A recent study by Professors Kinshuk Jerath and Klaus Miller provides experimental evidence about consumers' perceptions of privacy violations through the lens of the dual privacy framework.¹⁵ In their study, the authors present experimental subjects with different scenarios regarding data sharing and targeted advertising and ask them to rate the extent to which they perceive their privacy to be violated.

The authors consider a spectrum of scenarios that vary the level of intrinsic and instrumental values consumers are likely to experience, ranging from a behavioral targeting scenario (akin to the current practice in which consumers are targeted at the individual level and data leaves their devices), to a contextual targeting scenario (in which ads are targeted based on the content of the website the con-

12 When a consumer visits the sports magazine webpage, an auction is run to determine what ad to show to the consumer. Membership in the “mountain bike enthusiasts” audience can be one of the parameters used in the auction to select the most relevant ad. The main difference from current practice is that information about audience membership is stored on the consumer's device and the auction itself, as well, is run on the device. See *Protected Audience API overview*, Privacy Sandbox (January 27, 2022), <https://developers.google.com/privacy-sandbox/relevance/protected-audience>.

13 Recent academic research on PETs has examined their implication for research, studied their potential impact on advertisers and publishers, and documented the adoption of Privacy Sandbox technologies over time, but has not investigated consumers' perceptions. Policy discussions of PETs have also not examined consumers' perceptions. For example, in a report on PETs, the OECD discussed the potential of PETs to give consumers more control and protection over their data but did not address consumers' perceptions or expectations regarding PETs. Similarly, in a recent request for information, the U.S. Office of Science and Technology Policy stated that PETs present “a key opportunity to harness the power of data and data analysis techniques in a secure, privacy-protecting manner,” but did not mention how consumers may respond to or perceive them. The FTC also recently highlighted the possibility for firms to make false or misleading representations regarding PETs but made no reference to consumers' attitudes. See Garrett A. Johnson, Julian Runge & Eric B. Seufert, *Privacy-Centric Digital Advertising: Implications for Research, Customer Needs and Solutions* 9(1), 49–54 (2022); Miguel Alcobendas, Shunto Kobayashi, Ke Shi & Matthew Shum, *The Impact of Privacy Protection on Online Advertising Markets* (Working Paper, 2023); Garrett A. Johnson & Nico Neumann, *The Advent of Privacy-Centric Digital Advertising: Tracing Privacy-Enhancing Technology Adoption*, (Manuscript, March 21, 2024); *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, OECD Digital Economy Papers (March 8, 2023); *Request for Information on Advancing Privacy-Enhancing Technologies*, Science and Technology Policy Office (June 9, 2022); *Keeping Your Privacy Enhancing Technology (PET) Promises*, Federal Trade Commission (February 1, 2024).

14 Standard marketing practice suggests that firms must understand how consumers “think, feel, and act.” See Philip Kotler & Kevin Keller, *Marketing Management*, 15th Edition, Pearson (2016), p. 179.

15 Kinshuk Jerath & Klaus Miller, *Consumers' Perceived Privacy Violations in Online Advertising* (Working Paper, 2024).

sumer visits and nothing else), and a hypothetical scenario with no advertising and no targeting. Within this spectrum, the authors also consider two scenarios related to PETs, in which consumers' data does not leave their devices. In the first, consumers are targeted with ads at a group level based on interests (akin to Google's "Topics" technology discussed above), and in the second, they are targeted at the individual level (akin to Google's "Protected Audience" technology discussed above).

The authors find that consumers exhibit a small decrease in their perceived privacy violations under the PETs scenarios compared to the behavioral targeting scenario. More substantial declines in perceived privacy violations are observed for the contextual targeting scenario, both relative to the behavioral targeting scenario and the two PET scenarios. Additionally, the authors find that consumers only mildly prefer no ads to contextually targeted ads.

These findings suggest that privacy perceptions about user tracking and online advertising are affected less by the control users are given over whether/how the data is shared (does it leave the device?), and more by the expectations on how the data is used (is the data used to target ads effectively based on behavior?). This implies that while PETs may address concerns related to the intrinsic value of privacy, they may not fully address concerns pertaining to the instrumental value of privacy, and the latter may be large in magnitude.

In interpreting Jerath's and Miller's experimental findings, it is important to note that, in practice, consumers face a tradeoff between maintaining their information private and obtaining instrumental benefits from sharing that information. While Jerath's and Miller's study focuses on consumers' perceptions, these may be different from what might be inferred from revealed preference studies, i.e. analyses of consumer choices in the real world. For instance, it is well known that

consumers say that they value privacy highly but then give up their data relatively easily in exchange for a small benefit.¹⁶ This fact, known as the "privacy paradox," may then be resolved by recognizing that instrumental benefits of data sharing may actually outweigh the intrinsic disutility and instrumental costs associated with it.¹⁷ In other words, while consumers may perceive their privacy to be violated when surveyed, in practice, they may perceive the instrumental benefits they receive sufficient to justify sharing their information.

In the case of behavioral advertising (or other types of well-targeted advertising), these instrumental benefits include: (i) seeing advertisements for more relevant products and (ii) being able to access free content and services on websites or applications funded by advertising revenue. Academic research shows that ads produce higher revenue and better consumer responses when they can rely on third-party cookies that track users across sites. For example, Goldfarb and Tucker (2011) found that privacy laws that limited targeted advertising reduced user purchase intent by 65 percent.¹⁸ More recent research has found that publisher revenue would substantially decrease if third-party cookies were banned. For example, Alcobendas et al. (2021) find that publisher revenue would decline by 54 percent,¹⁹ and a 2019 study by Google found that publisher revenue would decline by 52 percent.²⁰ Lower revenue may reflect a reduced salience of the ads for consumers. In turn, lower revenue may adversely affect the quality and quantity of free content that publishers and app developers make available to consumers online.²¹

16 Patricia Norberg, Daniel Horne & David Horne, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, Journal of Consumer Affairs 4(1), 100-126 (2007); Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* (NBER, Working Paper No. 23488, 2017).

17 For example, a recent study finds a positive relationship between consumers' preference for privacy and the amount of information sharing they engage in. This finding suggests that even for the most privacy-sensitive consumers, the instrumental benefits of sharing information may outweigh the intrinsic and instrumental costs. See Long Chen, Yadong Huang, Shumiao Ouyang & Wei Xiong, *Data Privacy and Digital Demand* (Working Paper, 2024).

18 Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, Management Science 57(1), 57-71 (2011).

19 Miguel Alcobendas, Shunto Kobayashi, Ke Shi & Matthew Shum, *The Impact of Privacy Protection on Online Advertising Markets* (Working Paper, 2023).

20 Relatedly, the UK CMA replicated Google's results in a report published in 2020 using only UK users and found a decrease in publisher revenue as high as 70 percent. Deepak Ravichandran & Nitish Korula, *Effect of Disabling Third-Party Cookies on Publisher Revenue*, Google, 2019; Competition and Markets Authority, *Online Platforms and Digital Advertising: Market Study Final Report*, 2020.

21 Benjamin Shiller, Joel Waldfogel & Johnny Ryan, *The Effect of Ad Blocking on Website Traffic and Quality*, The RAND Journal of Economics 49(1), 43-63 (2018); Tobias Kircher & Jens Foerderer, *Ban Targeted Advertising? An Empirical Investigation of the Consequences for App Development*, Management Science 70(2), 1070-1092 (2023); Garrett A. Johnson, Tesary Lin, James C. Cooper & Liang Zhong, *COPPAocalypse? The YouTube Settlement's Impact on Kids Content* (Working Paper, 2024).

04

CONCLUSION

The findings of Jerath and Miller indicate that, as far as privacy perceptions are concerned, consumers care more about the outcome of targeted advertising rather than the process of how it comes about. This suggests that it may be helpful for firms to adopt a more consumer-centric approach that addresses concerns over how information is used rather than rely solely on the technical particulars of how information is processed. Further, realizing that, in practice, consumers face a tradeoff between keeping information private and obtaining instrumental benefits of sharing that information, firms may also want to take measures to educate consumers on privacy-enhancing technologies and initiatives being developed. In addition, firms may want to take steps to directly address consumers' perceptions about both the process of online advertising as well as its outcomes. Consumer education on privacy-enhancing initiatives may thus be useful in bridging the gap between technical definitions of privacy and consumers' perceptions.

Current regulatory initiatives focus primarily on the intrinsic aspects of privacy (control, collection, and data security). The findings of Jerath and Miller show that instrumental aspects of privacy (how the data are used for targeting, such as making inferences from it) also deserve importance in designing policy. Directions from policy-makers may prompt developers of future PETs to address instrumental concerns about privacy that current proposals do not seem to alleviate. ■

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.





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

by Peter Davis, Louise Freeman, Samid Hussain and Kate Scott¹

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 Google², YouTube³, Marriott⁴, Morrisons Supermarkets⁵, British Airways⁶ and easyJet⁷.

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 unauthorized access to, personal data in the UK⁸.

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 informa-

tion 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 unauthorized 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 of 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, GDPR Recital 82.

16, GDPR 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 Adjerd, 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.

Privacy by the Numbers: Economic Costs and Benefits of Privacy Regulation

[Vildan Altuglu](#), [Conor Foley](#), and [Lorenzo Michelozzi](#)

Aug 06, 2024 ⌚ 5 min read



Sezeryadigar via Getty Images

Policymakers and regulators have enacted laws and regulations in response to growing concerns about consumer privacy. This article reviews the economic literature on the effects of data privacy regulation on consumers and firms. This review is based on a May 2024 panel presentation hosted by the ABA Antitrust Section's Committee on Privacy and Information Security; Vildan Altuglu of Cornerstone Research moderated a discussion with Professor Avi Goldfarb of the University of Toronto and Professor Pinar Yildirim of the University of Pennsylvania. ¹

Two key insights emerge from our review of the existing literature. First, data exchanges between consumers and firms generate benefits and costs for both. Second, regulations that limit the collection and use of data to protect consumer privacy involve tradeoffs

between these costs and benefits, with consequences for competition and innovation. Stronger data privacy is not free.

Economic Framework for Analyzing Digital Privacy

The economic literature on digital privacy has analyzed information flows and examined the benefits and costs of such flows, as well as the economic impact of restrictions imposed on those flows.² The potential benefits and costs of information flows affect both consumers and firms. Digital technologies allow firms to collect and process consumer data, which can be used to provide insights about consumers, offer customers valuable products and services, develop sophisticated pricing strategies, or target advertising more effectively.³ Given these uses, flows of data – between consumers and firms and among firms – have the potential to create value for consumers and firms alike. However, consumers may prefer to restrict such flows because they have an intrinsic distaste for the collection and use of personal information or because they fear that it may lead to worse economic outcomes for themselves (e.g., higher prices).⁴ Firms also face costs to harness data flows. They need to develop adequate infrastructure to collect, store, and analyze data, and devote resources to protect data from cyberattacks and to comply with existing regulations. Accordingly, an economic understanding of privacy needs to consider the benefits and costs associated with data flows and evaluate the tradeoffs that arise from restricting these flows.

In addition to direct costs and benefits to consumers and firms, an economic understanding of privacy needs to consider certain economic features that are peculiar to data flows. Data sharing can cause spillovers to third parties, leading to both positive and negative externalities. A positive externality could be innovation based on insights drawn from new data.⁵ A negative externality could arise when one person shares data that reveals information about others.⁶ Solutions to externalities that rely on assigning property rights are difficult to implement in practice in the digital domain.⁷ In addition, businesses that collect and analyze data may be subject to economies of scale and scope that give rise to competitive concerns.⁸

Empirical Evidence on Effects of Privacy Regulation

Multiple studies have evaluated the impacts of privacy regulations on firms and consumers. A pioneering 2011 study by Avi Goldfarb and Catherine Tucker examined the impact of the European Union (EU) ePrivacy Directive.⁹ Implemented in 2004, this directive imposed rules that limited the types of data advertisers could use to target ads

in the EU. Using data on advertising campaigns inside and outside the EU, the study showed a significant decrease in the effectiveness of banner ads – as measured by changes in survey respondents' stated purchase intentions – following the directive's implementation. These results suggest that the regulation functioned as intended: firms likely used less data to target ads, which in turn made ads less effective. At the same time, reduced advertising effectiveness may have resulted in less relevant ads for users and may have hampered the growth of the online advertising industry in Europe relative to the United States.¹⁰

Additional evidence about the costs of privacy regulation has emerged from academic research that examines the impact of the EU General Data Protection Regulation (GDPR). Implemented in 2018, the GDPR is one of the most significant privacy regulations enacted to date. Empirical studies of the effects of GDPR have documented outcomes that are consistent with a reduction in data flows, accompanied by potentially adverse economic outcomes. For example, using a multi-country consumer panel, Zhao et al. (2023) finds that, post-GDPR, EU consumers expended greater effort in online searches – as measured by total time spent, number of search terms, or number of sites and domains visited in a given search session – without substantial changes in their purchasing behavior, suggesting that the efficacy of consumers' online searches had decreased.¹¹ Zhao et al. (2023) also finds that, post-GDPR, EU consumers became more likely to visit and purchase online from larger firms rather than smaller ones, suggesting that larger firms may have benefitted from less effective searches while smaller firms may have been left at a competitive disadvantage.¹² Goldberg et al. (2024) studies the effect of GDPR using website analytics and documents reductions in e-commerce revenue, post GDPR, with more pronounced effects for smaller firms.¹³ Other studies looking at the effect of GDPR on firms find reduced investment,¹⁴ fewer new app launches,¹⁵ and a softening of competition in the online advertising market in favor of large incumbents.¹⁶ Evidence on direct consumer benefits from the increased privacy protections of GDPR has, so far, proven to be more elusive, as these benefits are hard to evaluate empirically with the type of data available to researchers.¹⁷

Researchers have also analyzed regulatory changes in the United States, in particular the 2019 settlement of an enforcement action involving a large technology firm under the federal Children's Online Privacy Protection Act (COPPA), and the 2020 introduction of the California Consumer Privacy Law (CCPA). The findings emerging from this literature, which examines the economic consequences of these changes rather than direct privacy benefits for consumers, are broadly consistent with what has been learned from the experience of the GDPR. Privacy regulations can reduce the flow of data but can be accompanied by lower innovation,¹⁸ reduced consumer choice, and less

personalization.¹⁹ In addition, regulations can have differential effects on firms, with gains in market shares for firms that are better equipped to face the new regulatory environment.²⁰

Conclusion

Both economic theory and recent empirical studies of the effects of privacy regulations point to a tradeoff between strengthening privacy protections and incurring costs in terms of reduced competition, innovation, and consumer choice relating to digital products. The findings from existing economic research can help policymakers understand these costs and benefits better and help them with the complex balancing act between protecting privacy and the potential drawbacks of restricting data flows. Future research can illuminate these costs and benefits further and assess how they may change as technological capabilities continue to improve (e.g., with the development of new privacy-enhancing technologies) and as privacy regulations evolve.

The views expressed herein are solely those of the authors, who are responsible for this content, and do not necessarily represent the views of Cornerstone Research.

Endnotes

1. A video of this panel presentation is available at https://www.americanbar.org/groups/antitrust_law/resources/on-demand/privacy-by-the-numbers/.
2. [Goldfarb, Avi and Que, Verina F. \(2023\) "The Economics of Digital Privacy," *Annual Review of Economics*](#).
3. Agrawal, Ajay, and Gans, Joshua, and Goldfarb, Avi. (2022) "Power and Prediction: The Disruptive Economics of Artificial Intelligence," *Harvard Business Review Press*.
4. Economists refer to these motives as an "intrinsic" and an "instrumental" value for privacy. See, for example, Lin, Tesary (2022) "Valuing Intrinsic and Instrumental Preferences for Privacy," *Marketing Science* Vol. 41 No. 4 pp. 663-869.
5. Jones, Chad and Tonetti, Christopher (2020) "Nonrivalry and the Economics of Data," *American Economic Review* Vol. 110 No. 9 pp. 2819-2858.

6. Goldfarb, Avi and Que, Verina F. Que (2023) "The Economics of Digital Privacy," *Annual Review of Economics*, p. 267-286.
7. For example, Dosis and Sand-Zantman (2022) develop a model in which assigning property rights do not alleviate concerns about data sharing due to contracting frictions. See Dosis, Anastasios and Sand-Zantman, Wilfried (2022) "[The Ownership of Data](#)," *The Journal of Law, Economics, and Organization* Vol. 39 No. 3 pp. 615-641.
8. Large up-front costs to amassing large and diverse datasets or developing tools for analyzing such datasets may favor large incumbent firms and limit the competitive constraint from smaller rivals and potential entrants. See Furman, J., Coyle, D., Fletcher, A., McAuley, D., and Marsden, P. (2019) "Unlocking digital competition: Report of the Digital Competition Expert Panel," UK government publication, HM Treasury, available at <https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel>. Research has also emphasized that there may be limits to economies of scale in data processing. See, for example, Bajari, Patrick et al. (2019) "The Impact of Big Data on Firm Performance: An Empirical Investigation," *AEA Papers and Proceedings* Vol. 109 pp. 33-37.
9. Goldfarb, Avi and Tucker, Catherine E. (2011) "Privacy Regulation and Online Advertising," *Management Science* Vol. 57 No. 1 pp. 57-71. The United Kingdom implemented the ePrivacy Directive first in December 2003.
10. Goldfarb, Avi and Que, Verina F. (2023) "The Economics of Digital Privacy," *Annual Review of Economics*, Vol. 15 pp. 267-286 at p. 280.
11. Zhao, Yu and Yildirim, Pinar and Chintagunta, Pradeep (2023) "Privacy Regulations and Online Search Friction: Evidence from GDPR," Marketing Science Institute Working Paper Series Report No. 23-141.
12. Zhao, Yu and Yildirim, Pinar and Chintagunta, Pradeep (2023) "Privacy Regulations and Online Search Friction: Evidence from GDPR," Marketing Science Institute Working Paper Series Report No. 23-141.
13. This larger reduction in revenue for smaller firms occurs in part because consumers are less likely to opt into data sharing with smaller firms and more likely to do so with larger firms. See Goldberg, Samuel G. and Johnson, Garret A. and Shriver, Scott K. (2024) "[Regulating Privacy Online: An Economic Evaluation of the GDPR](#)," *American Economic Journal: Economic Policy* Vol. 16 No. 1 pp. 325-358.
14. Jia, Jian and Jin, Ginger Zhu and Wagman, Liad (2021) "[The Short-Run Effects of General Data Protection Regulation on Technology Venture Investment](#)," *Management Science* Vol. 40 No. 4 pp. 661-684.

15. Janssen, Rebecca and Kesler, Reinhold and Kummer, Michael E. and Waldfogel, Joel (2022) "GDPR and the Lost Generation of Innovative Apps," NBER Working Paper No. 30028.
16. Peukert, Christian et al. (2022) "[Regulatory Spillovers and Data Governance: Evidence from the GDPR](#)," *Marketing Science* Vol. 41 No. 4 pp. 746-768.
17. Further, while an experimental study conducted prior to the implementation to the GDPR documented that study participants were willing to pay for the data rights offered under GDPR, other studies conducted post-GDPR found limited changes in consumer awareness or exercise of privacy protections, with only a small percentage of consumers appearing to opt out of data collection online. See Johnson, Garrett A. (2023) "Economic research on privacy regulation: Lessons from the GDPR and beyond," Working paper, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4290849, pp. 1, 18-19, 32; Sobolewski, Maciej and Palinski, Michal (2017) "How much consumers value on-line privacy? Welfare assessment of new data protection regulation (GDPR)," University of Warsaw Faculty of Economics Sciences Working Paper No. 17/2017 (246); Presthus, Wanda & Sorum, Hanne (2021) "A three-year study of the GDPR and the consumer," in *14th IADIS International Conference Information Systems 2021*, available at <https://www.iadisportal.org/digital-library/a-three-year-study-of-the-gdpr-and-the-consumer>; Goldberg, Samuel G. and Johnson, Garret A. and Shriver, Scott K. (2024) "Regulating Privacy Online: An Economic Evaluation of the GDPR," *American Economic Journal: Economic Policy* Vol. 16 No. 1 pp. 325-358.
18. Canayaz, Mehmet et al. (2022) "Consumer Privacy and the Value of Consumer Data," Swiss Finance Institute Research Paper Series No. 22-68.
19. Following the settlement of a COPPA enforcement action involving a large technology firm, Kircher and Foerderer (2023), Kircher and Foerderer (2024), and Johnson et al. (2024) analyze changes for businesses producing digital content for children. These papers find a shift toward non-affected (i.e., non-child and non-advertising-supported) business lines and an overall decline in child-directed content. See Kircher, Tobias and Foerderer, Jens (2023) "Ban Targeted Advertising? An Empirical Investigation of the Consequences for App Development," *Management Science* Vol. 70 No. 2 pp. 1070-1092; Kircher, Tobias and Foerderer, Jens (2024) "Does Privacy Undermine Content Provision and Consumption? Evidence from Education YouTube Channels," Working paper, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4473538; Johnson, Garrett et. al. (2024) "COPPAcalypse? The Youtube Settlement's Impact on Kids Content" Working paper, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4430334.
20. For example, studying firms in the voice AI market, Canayaz et al. (2022) find that, post-CCPA, firms that have the scale and capabilities to collect their own data to develop new products and train their algorithms saw greater investment and increases in market share relative to firms relying on third-party data. See Canayaz, Mehmet et al. (2022) "Consumer Privacy and the Value of Consumer Data," Swiss Finance Institute Research Paper Series No. 22-68. Further, two studies – Doerr et al. (2023) and Gupta et al. (2023) – examine the impact of CCPA on the

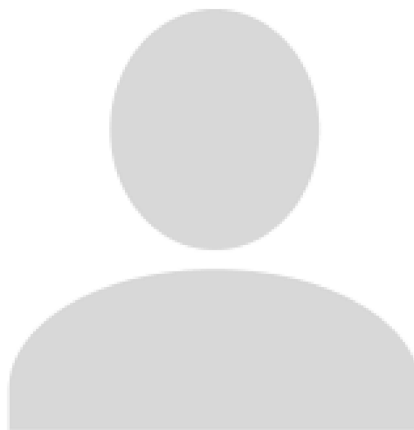
California mortgage market and find lending shifting away from banks and into fin tech firms, with fin techs having regulatory and technical advantages under the laws compliance rules. See Doerr, Sebastian et al. (2023) "Privacy regulation and fintech lending," BIS Working Papers No. 1103; Gupta, Manish et al. (2023) "The Cost of Privacy. The Impact of California Consumer Protection Act on Mortgage Markets," Swiss Finance Institute Research Paper Series No. 23-25.

Authors



Vildan Altuglu
Cornerstone Research

...



Conor Foley

...



Lorenzo Michelozzi
Cornerstone Research

...

Published by the American Bar Association ©2025. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

ABA American Bar Association |

https://www.americanbar.org/groups/antitrust_law/resources/newsletters/privacy-by-numbers-economic-costs/