Case Notes

A Market Perspective on a Ruling about Data Markets

February 2019

This article examines a key decision concerning the all-important data market. My purpose is not to provide a comprehensive analysis of the ruling in the case, but rather to explore parts of the ruling that I find troubling from an economic perspective. I also discuss potential implications for conduct in the data markets, and for the future of collective actions. [a]

Late last year, the London High Court dismissed the claims brought in *Lloyd v. Google,*[b] in a ruling that may frustrate consumers and economists alike.[c]

In the case, Google was accused of surreptitiously tracking and collecting iPhone users' data.

Apple's Safari browser had been set, by default, to block third-party cookies.[d] Google allegedly exploited a loophole it found in the browser settings and, over a period spanning a few months in 2011-2012, placed its own third-party cookies on iPhone devices, without iPhone users' knowledge or consent, to track users' internet activity through their browser-generated information ("BGI").

Consumer advocate Richard Lloyd sought to represent a class of individuals comprising Apple iPhone users (the "Claimants"), alleging that Google's tracking, collating and selling of the users' accumulated data, to advertisers, breached the duty imposed by §4(4) of the Data Protection Act 1998 ("DPA").[e]

AUTHOR

Gene Phillips
Director
gene.phillips@pf2se.com

[a] Although there are differences, I use the terms "collective action," "representative action" and "class action" interchangeably.

[b] *Lloyd v. Google LLC* [2018] EWHC 2599 (QB). Neither the author, nor PF2, has any connection to, or vested interest in, this case.

[c] The ruling might unfairly suggest that large technology companies can trample on consumers' privacy rights, without any legal consequence.

[d] A cookie is a small data file that is sent from a website to a user browsing the website, and stored on the user's device. Cookies were designed to remember information while a user browses, such as which items have already been added to a virtual shopping cart in an online store. Third-party cookies are mostly aimed at tracking users' activity across multiple websites, and often allow the compiling of long-term records containing users' browsing histories. (See ruling at [10].)

[e] The Claimants asserted that Google's tracking and collating of iPhone users' BGI enabled Google to obtain or deduce information not only about their online habits and location, but also about personal details including their race or ethnicity, social class, political or religious views, age, health, gender and financial position. (See [11].)

The Court ultimately ruled that the Claimants failed to adequately claim damages under the DPA. The Court also found that it was improper to litigate this case as a class action.[f]

I will examine the problematic parts of the Court's reasoning here. While I do not necessarily disagree with the result of the case, the Court's assumptions concerning data markets are troubling, as is the determination that Claimants could not proceed as a class.

Dismissal Based on Damages — Three Main Factors

Claimants sought damages for: (i) the commission of the wrong itself; (ii) the infringement of Claimants' data protection rights; and (iii) Claimants' loss of control over their personal data. [23]

The Court dismissed the lawsuit in its entirety, for failing to claim damages that are recoverable under the DPA. The Court's analysis drew regularly on three factors to distinguish this case from those favorable to Claimants:

1. Claimants' Failure to Allege *Distress*. Claimants failed to allege that they suffered any form of distress owing to Google's tracking of their internet activity.
2. Claimants' Failure to Allege *Financial Loss*. Claimants failed to allege that they suffered any financial loss caused by Google's alleged misconduct.[g]
3. Claimants' Failure to *Individualize* Damages. Claimants sought an "equal, standard, 'tariff' award" as compensation for all members of the putative class.[h]

Although these three factors formed the main basis for dismissal, I do not focus on them extensively in this article because they are, at their essence, legal reasons for dismissal.

More interesting to us non-lawyers are those parts of the Court's ruling that may determine future conduct in data markets. I mention the damages factors so that we can recognize their occasional influence on the Court's analysis in denying Claimants' effort to litigate collectively a class.

---

[f] By comparison, the U.S. Federal Trade Commission imposed a record fine of $22.5m on Google – the highest amount ever levied by the Commission on a single entity – for the alleged misconduct at issue here. Google also settled similar claims, brought by 37 U.S. states and the District of Columbia, in the amount of $17m. (See [13].)

[g] At [76], the Court quotes from a prior case: "[The DPA] entitles [Claimants] to compensation for *pecuniary damage* and *distress* .... [The DPA] does not give [Claimants] a cause of action based upon a misuse of data which does not actually cause [them] to suffer [pecuniary] damage or distress but rather allows [Google] to profit ...." In other words, the Court is saying that it is insufficient to allege only that Google profited from Claimants' data – Claimants must also show that they were damaged.

[h] "No specific figure is put on the tariff, though ranges are mooted, and a figure of £750 was advanced in the letter of claim." [3] Claimants' approach, in seeking *equal* damages for each Claimant, was unfortunate and a significant factor in the Court's rejection of the claims. (See [74].) Claimants may have decided that pursuing equal damages would be more efficient, avoiding the seemingly burdensome task of calculating damages borne by each of the millions of individual users. Claimants' disposition can usually be alleviated, at modest expense, by employing statistical methods to provide individualized damage *estimates* (without the need for detailed litigation discovery).

The Court's Rejection of the Class

In rejecting the arguments for a representative action, the Court's reasoning focused heavily on differences among the individual Claimants. I divide the core differences into two categories.

Differences in data quality: Some iPhone users are more active on their cell phones than others, and therefore generate more data (or a richer data set) for Google to use, analyze or sell. (See [91].)

Differences in attitudes: Users have various attitudes towards the acquisition and disclosure of their data. (See [80].) The Court surmised that if users had been asked to accept Google's third-party cookies, some would have consented while others would have refused.

> *"I do not believe that the authorities show that a person whose information has been acquired or used without consent invariably suffers compensatable harm, either by virtue of the wrong itself, or the interference with autonomy that it involves. Not everything that happens to a person without their prior consent causes significant or any distress. Not all such events are even objectionable, or unwelcome. Some people enjoy a surprise party. Not everybody objects to every non-consensual disclosure or use of private information about them. Lasting relationships can be formed on the basis of contact first made via a phone number disclosed by a mutual friend, without asking first."* [74][i]

The Court rejected Claimants' allegation of equal damages, given the differences among the iPhone users. The Court explained further that these *data quality* and *attitudinal* differences were not only at odds with the notion of equal damages, but at odds with the notion that Claimants had enough in common to proceed as a class; the Court ruled that a representative action was therefore inappropriate.

> *"… the question of whether or not damage has been sustained by an individual as a result of the non-consensual use of personal data about them* ***must depend on the facts of the case****. The bare facts pleaded in this case,* ***which are in no way individualised****, do not in my judgment assert any case of harm to the value of any claimant's right of autonomy that amounts to "damage" within the meaning of DPA s 13."* [74, with emphasis added]

> *"… it cannot be supposed that the breach of duty or the impact of it was uniform across the entire Class membership; on the contrary, it is inevitably the case that the nature and extent of the breach and the impact it had on individual Class members will have* ***varied*** *greatly."* [92, with emphasis added]

> *"… a representative action would not be legitimate because those claimants who had suffered "damage" would have* ***different interests from one another****, dependent on the* ***individual facts of their cases****."* [89, with emphasis added]

The Market Objects! Market-Based Arguments Favor a Class Action

The Court's primary concerns were that: some Claimants were heavy internet users, creating a rich set of BGI, while others surfed the web less frequently (*data quality* differences); and some users would have allowed cookies, had they been asked, while others would have refused (*attitudinal* differences).

[i] I am not convinced by the Court's analogy here: it risks conflating social norms with commercial considerations. Surprise parties with friends – or connections made based on a mutual and friendly reference – are governed by conventions that seldom overlap with those governing commercial relationships.

Can all of these users really be part of the same class? The answer, I believe, is a resounding "Yes."

The short explanation is that data, like gold or oil, is a traded product. Differences in data quality are readily accommodated in market prices; and those prices are entirely agnostic to any differences in their owners' attitudes.

Data Quality Differences Should Not Disqualify a Class

Some Claimants may have owned their iPhones throughout the period of alleged misconduct, generating a richer and more comprehensive data set than that of other Claimants who bought their iPhones only during the final week of the relevant period. In that sense each Claimant is different: some would have higher damages than others. But this distinction does not make a class action any less appropriate, and it certainly does not translate into different interests, among the Claimants, regarding the *outcome* of the litigation.

In most securities class actions, for example, the class comprises shareholders of the corporation being sued. The fact that each shareholder may hold a different number of shares in the corporation, and is therefore entitled to a different amount of damages, does nothing to differentiate the shareholders' interests in the litigation or its outcome.[j]

Differences in Attitude Should Not Disqualify a Class

Capital markets work well precisely because everybody can and does have a different opinion. Firms and individuals buy and sell stocks, but that does not mean they evaluate the same stocks in the same manner – in fact they all disagree about value, which is why trading occurs. Those who believe a certain stock is cheap (or relatively cheap) might buy at the current price, while those who believe it is overvalued might sell.

The value of each user's data is, similarly, an amount certain *in the marketplace*, irrespective of whether the user has a carefree attitude towards her data or cherishes that data and guards it carefully. Some examples might help to clarify my point:

- A thief who steals $50 from a rich person and a poor person damages both people equally, regardless of any differences in their attitudes towards the $50.
- Most basic economics textbooks describe the concept of *diminishing returns*: for someone buying a hamburger, the first hamburger may have greatest utility but the second and third, if eaten in quick succession, will be less tasty and desirable – perhaps even turning from being an asset into a liability. Here, the fact that one has already eaten one's first hamburger is entirely irrelevant to the price of hamburgers. Each restaurant offers its hamburgers at a specific price that ignores each *individual's* marginal utility function or benefit.
- Consider a large quantity of gold (or oil or any valuable commodity). In comparison to the individual punter, money-center banks like Barclays or JPMorgan would have greater utility for a large quantity of gold, being better positioned to store the gold (and protect it!) and better equipped to sell large quantities at or near the current market price. The individual punter might be a forced seller, with prospective buyers taking advantage of her perceived inability to store the gold and her limited access to willing buyers at market prices. Thus, the individual punter would on average sell her gold for a lesser amount than a money-center bank. But this realization does not impact the market's ability to

[j] Those with higher damages can easily be accommodated by allocating them a larger share of any settlement amount.

price gold: there is a market for gold and a price at which it trades. In this sense, the market is agnostic to whether JPMorgan owns the gold, or you or me; and it is agnostic to the owner's attitude towards the gold.

People, by their very nature, have different attitudes and opinions about everything. (The joke goes: four people, five opinions.) Markets, thankfully, allow for consolidated prices, regardless of people's attitudes. Data markets are just one market. Your or my attitudes towards data are irrelevant. It does not matter whether you value data, nor what you might do with your data if I asked you to give it up. The issue is what the data is worth *in the marketplace* – not what it is worth *to you*.

Altogether, Claimants' attitudes towards their data, its importance, its value, or their rights with respect to it, are all of no consequence when testing the similarity of their interests in the proposed litigation.

The Court's Assumptions about Data Markets May Set Bad Precedent

The Court rejected the assessment of damages based on the amount users would have charged Google for their personal data, in a *hypothetical negotiation* in which Google would have bargained with users for their data. The Court stated: "It is hard, if not impossible, to envisage the bargain which this approach requires the court to hypothesise." [78]

I am troubled by the Court's analysis, because I find it fairly easy to envisage ways in which a hypothetical negotiation may have occurred, as I will explain. For the purposes of discussion, I break the Court's analysis into three parts:

> *"The claim is put on the basis that the gist of the wrong is a 'loss of control' over information - control which the members of the Class would not willingly have given up. It is hard, if not impossible, to envisage the bargain which this approach requires the court to hypothesise. (1)* ***It would not, indeed could not, be an individualised affair****. It could only be a process by which each individual was given the chance to opt in to the use of his or her personal data on standard terms set by Google. (2) Such bargains do of course take place, millions of them, every day.* ***But they do not involve the offer or payment of any money****."* [78, with numbering and emphasis added]

> *"For the reasons I have given, it seems to me to be wholly artificial to envisage a bargaining process involving such individuals. The only option realistically open to them would be to refuse consent. (3) But if that is wrong, then* ***it is not possible to envisage <u>the same negotiation</u> in the case of every claimant. Their personal characteristics and attitudes to data disclosure will inevitably differ.*** *The extent to which they would be willing to consent, and their readiness to accept any given sum of money in return, will vary."* [80, with numbering and emphasis added]

<u>Part (1)</u>. The Court asserts that any hypothetical "bargain" could not be "an individualized affair" and would need to be standardized: "It could only be a process by which each individual was given the chance to opt in to the use of his or her personal data on standard terms set by Google."

<u>Part (2)</u>. The Court assumes that standardized bargaining cannot involve money. "Such bargains do of course take place, millions of them, every day. But they do not involve the offer or payment of any money."

I disagree with the Court here, and the implications are important because the Court's analysis rests on the assumption that standardized bargaining cannot involve money.

Shopping is an excellent example of standardized bargaining that involves money. Clothing and grocery stores habitually offer products at set prices to all consumers. The Court could likewise have contemplated a hypothetical bargain in which Google offered a fixed payment to each user, which could either be accepted or rejected.

Part (3). The Court assumes that standardized bargaining must take users' different attitudes into account. The Court explains that it cannot conceive of any standardized bargaining process that does this: "it is not possible to envisage the same negotiation in the case of every claimant. Their personal characteristics and attitudes to data disclosure will inevitably differ."

I disagree. It is easy for standardized bargaining to take users' different attitudes into account. Stock markets and grocery stores function well every day, and market prices shift to accommodate users' different interests. If kale is fashionable it may sell out, or a store may lift its price. If kale is overpriced, few would buy it, and the market would lower the price — but the "same negotiation" would still occur with all consumers, only at a different price level.

Users' different attitudes toward data do not preclude standardized bargaining for data any more than their different attitudes towards kale preclude grocery store from offering it to them at the same price. Different attitudes do not impair the ability for standardized prices – they simply inform markets in getting to the right price.

The Court misses a simple solution: that Google could offer a basic, fixed payment to each user in exchange for users' data. The "same negotiation" can take place. Users' attitudes simply help shape the price level in the negotiation.

Tailored, Individualized Negotiation – No Problem!

The Court seems to require that the hypothetical negotiation account for users' different attitudes. This poses no concern in today's world, and certainly not for Google.

Google could tailor algorithms that "negotiate" with each user, taking into account each user's attitude. This is common in commercial markets. When purchasing an airline ticket (or similarly when renting a car or a hotel room) consumers decide which day to fly, whether to fly business class or economy, and whether to pay for luggage in advance. These are all attitudinal differences, taken into account in the negotiation (by the seller's algorithm) in arriving at the ultimate price, based on each consumer's specific preferences.

Google could similarly "negotiate" with users by offering them different prices for each distinct piece of user information. Users could agree to accept payment in return for being tracked, or opt out of all tracking or some tracking they find to be mispriced or objectionable. Trusting users, or those with a healthier risk appetite, may well opt in to most or all tracking in exchange for the compensation offered, while others may be more circumspect and may demand a richer return (or reject third-party cookies regardless of the offer).

Such a "pay-for-data" system would be both a tailored, and a money-based bargain; and it would seem to be a fair system.[k] This is how markets function.

Contrary to the Court's analysis, my experience with capital markets leads me to believe that "pay-for-data" systems can adequately compensate users for their data and I hope and expect them to become the norm. For example, the *Facebook Research* application reportedly paid users up to $20 per month, plus referral fees, for allowing Facebook to track their online activities.[l] Several companies – including Wibson, BitClave, Datum and the Tide Foundation – are working on applications that enable individuals to manage and monetize their personal data, rather than giving it up freely.

The "Implicit Bargain" is No Bargain

The most apt hypothetical negotiation the Court could envisage was an "implicit bargain" in which users exchange their data for targeted advertisements.[m]

> *"… the **implicit bargain** is that if the consumer consents to the acquisition and use of their personal data in the ways set out in the "privacy notice" or "cookie notice", **the consumer will receive something else of value, in the form of targeted or filtered communications**, more likely to be of interest to the consumer than if consent was withheld. The only alternative on offer is the refusal of consent."* [78, with emphasis added]

In formulating the "implicit bargain," the Court rightly acknowledges that users' data is a valuable asset: in exchange for it, "the consumer will receive something else of value." But the Court seems to suggest that Claimants would suffer no damages in this "bargain," because they would have received something of value in return for their data – targeted advertisements.

While the Court does not necessarily endorse this "implicit bargain," I am opposed to it, and wish to deter courts from considering such a "bargain" in the future.

The "Implicit Bargain" Has Some Unhappy Surprises

Inherent in the Court's "implicit bargain," is the assumption that users receive *only* targeted advertisements – and nothing else – in exchange for their data. But how do we know that users' data is not exchanged for targeted advertisements *plus* spam (for example)? At the very least, the exchange of

---

[k] Whether such a negotiation is considered "individualized," because it can be different for different users, or whether one considers it to be "standardized," because the same determinative algorithm does the "negotiation," is only a matter of semantics that carries no consequence here.

[l] Apple took issue with the *Facebook Research* application, asserting that it breached Apple's policies. Facebook reportedly defended its actions. According to the *Financial Times*, a Facebook spokesperson said: "Despite early reports, there was nothing 'secret' about this; it was literally called the Facebook Research App. It wasn't 'spying' as all of the people who signed up to participate went through a clear onboarding process asking for their permission and were paid to participate." (See here.)

[m] The Court recognizes that the "implicit bargain" is imperfect because, as the Court notes, some users would have refused to participate in the bargain in the first place. The "implicit bargain" considers only the damages suffered by those users who would have participated, but the real concern is those users who would have refused to enter the bargain. The "implicit bargain" also assumes away a key problem: that the right to choose whether to bargain at all – a fundamental right in a commercial relationship – is taken away from users.

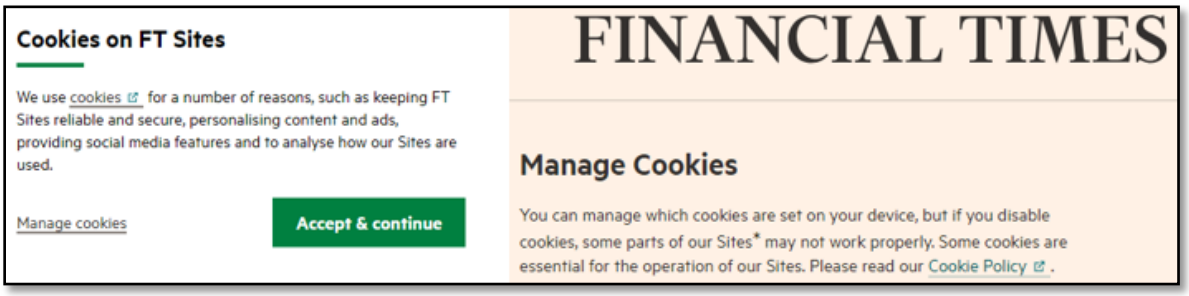
one's personal data exposes one to a host of risks, such as identity theft and price discrimination.[n] This is a rather unhappy consequence for the "implicit bargain," because it means that the hypothetical exchange is not as simple as trading one thing *of value* for another.

Even if Google were to have asked users to "Accept Google's Third-Party Cookies," the nature of such a "bargain" would typically be unknown to users.

While I have not tested the following hypotheses, I am confident that if we were to survey a random group of iPhone users today – and certainly back in 2011-2012 at the time of the alleged misconduct – we would find that users:

- mostly do not know what *cookies* are;
- cannot distinguish between *first-party cookies* and *third-party cookies*;[o]
- do not know to what extent they are being tracked when accepting cookies;
- often correctly believe that if they refuse cookies, their ability to access the website at hand will be impaired (see Graphic 1); and
- would more regularly refuse if meaningful terminology were used: if users were asked whether they agree *"to be tracked"* (which sounds relatively ominous, but is accurate), they would more regularly refuse than if asked "*to accept cookies*" (which sounds, artfully, innocuous).

Graphic 1 – Snapshots Concerning Cookies, From the *Financial Times'* Website
February, 2019



This graphic shows how websites typically handle cookies. Websites do not ask: "Accept cookies in exchange for tailored advertising?" They ask only if users will agree to accept cookies. The green button "Accept & continue" suggests that one must accept cookies to proceed to the website — there is no button that reads "Refuse & continue" — but in my tests I was able to continue with the site without accepting cookies. The *FT* states that cookies are used "for a number of reasons," not all of which are necessarily provided. Targeted advertisements are not the *sole* consequence of "accepting and continuing," but the personalizing of "content and ads" is disclosed here, among other reasons.

In a separate but not dissimilar case, the French data authority National Data Protection Commission ("CNIL") imposed a fine on Google in accordance with the General Data Protection Regulation ("GDPR").

[n] I describe these risks and others in further detail subsequently in the article.

[o] First-party cookies are created by the website being visited, allowing the website to track a user's activity as the user moves from page to page within the website. Third-party cookies, sometimes called "tracking cookies," track users' activity across multiple websites, allowing the compilation of long-term records containing users' browsing histories. Most web browsers come with first-party cookies enabled. But third-party cookies are often considered a greater security threat and an invasion of privacy. That is presumably why the default setting on Apple's Safari browser was to block third-party cookies. (See [10].)

CNIL noted that Google's requests for user consent were insufficient in that users "are not able to fully understand the extent of the processing operations carried out by GOOGLE," and "the information communicated is not clear enough so that the user can understand that the legal basis of processing operations for the ads personalization is the consent, and not the legitimate interest of the company."[p]

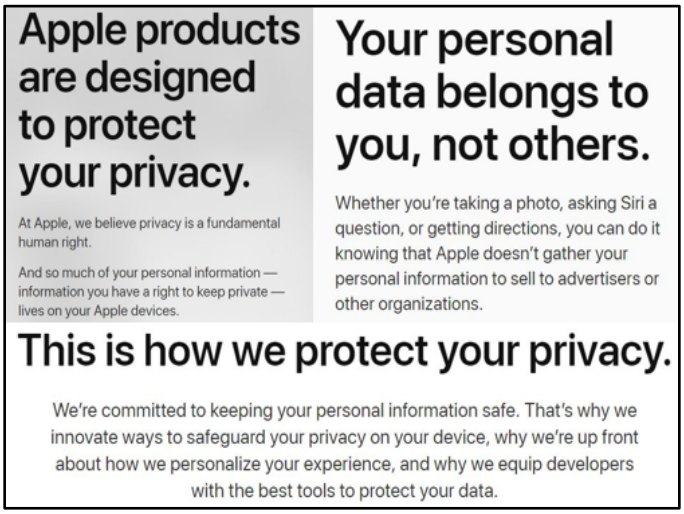
User Beware: Targeted Advertising is No Benefit

I am not aware of any market in which consumers pay to improve the quality of the advertisements they receive. However, markets do exist in which consumers pay to avoid being tracked or to decrease the number of advertisements they receive. Anti-spyware companies, for one, help users delete third-party cookies.[q]

Also, as noted in the ruling at [10], Apple's default setting was to block third-party cookies, which shows that Apple considers third-party cookies to be a problem – not a benefit. In fact, Apple recently adopted a marketing slogan to emphasize privacy as a core benefit of owning an iPhone: "What happens on your iPhone, stays on your iPhone."[r] (See also Graphic 2.)

Third-party cookies present not only a privacy problem, but also a performance problem for those websites allowing them. According to one study, target-based advertising has the disadvantage of causing websites to load more slowly, with increased delays that can exceed two seconds.[s]

Graphic 2 – Snapshots from Apple's Website (Feb. 2019)



Altogether, it is debatable whether targeted advertisements are of any benefit at all. On the other hand, privacy is certainly valuable and the market for privacy is well established.

The Court Disapproves of Class Actions — a Valuable Tool for Market Correction

The Court had two key concerns: *first*, the claim did not give rise to damages (if any) under the DPA; and *second*, the nature of the damages suffered varies from user to user. With these concerns in mind, the Court dismissed the case and held that a class action was improper:

[p] See here.

[q] Back in 2007, for example, the anti-spyware team at CA Technologies was reportedly instrumental in exposing Facebook for collecting personal information about their users, without their knowledge, even when those users had opted out of Facebook's *Beacon* online advertisement program and were not logged in to Facebook's website. (See here and here.) After settling a class action, Facebook terminated *Beacon*. (*CA Anti-Spyware* was a spyware detection program, and is presently available as *Total Defense Anti-Virus*. Prior to 2007 it was known as *PestPatrol*.)

[r] See here.

[s] See here.

"The conclusions are, in summary, that:

1. *The essential requirements for a representative action are absent. The Representative Claimant and the Class do not all have the "same interest" within the meaning of CPR 19.6(1).*
2. *Even if the Class is appropriately defined, there are insuperable practical difficulties in ascertaining whether any given individual is a member of the Class.*
3. *Further and alternatively, the Court's discretion would in any event be exercised against the continuation of the action as a representative action."* [82]

The Court's ruling cites to four central propositions, submitted by Claimants, which define the conditions for meeting the "same interest" test.

1. *"Persons have the 'same interest' if they have a common interest and a common grievance.*
2. *Persons may have the same interest in a claim even if there are disagreements between them and even if the quantum of damages that they have suffered is different.*
3. *A representative claimant may represent a class, even if the members of that class have been affected by the defendant's actions in different ways.*
4. *There is no limit to the number of persons that can be within the class to be represented."* [85]

The Court rejected these arguments, but without providing clear justification.[t]

"The first three of these propositions give rise to dispute. Google submits that the existence of a common grievance against the same defendant is not enough to satisfy the 'same interest' condition. In particular, where the defendant is alleged to have damaged individual rights and interests, the representative action will be unavailable unless every member of the class has suffered the same damage (or their share of a readily ascertainable aggregate amount is clear). Further, and in any event, the procedure will be unavailable where different potential defences are available in respect of claims by different members of the class. I accept Google's submissions, and in my judgment these principles apply to the facts of this case, so as to disqualify this claim." [86]

I have argued throughout that the differences among Claimants – in data quality, attitudes and amount of damages – are irrelevant to the commonality of their interests. With that said, my expectation is that the Claimants would in fact satisfy the condition, as described by the Court, that "every member of the class has suffered the same damage (or their share of a readily ascertainable aggregate amount is clear)."[u]

[t] Among other things, it is unclear: (1) what the Court means by "the same damage," and why the Court insists on it; and (2) what different defenses Google might be able to raise in relation to some but not all Claimants, or how or why the ability to raise different defenses conflicts with Claimants' four propositions.

[u] The standard, per my reading, is *same interest* – not *identical circumstance*. If a class action required that each class member be *identical,* many class actions would be precluded. This is one reason courts employ guideline rules to determine the suitability of class actions (such as the "same interest" test) rather than rigid bright-line rules.

Common Interests and Common Grievances: Exposure to Undue Risk

While Claimants did not allege that they suffered any form of *distress* owing to Google's tracking of their internet activity, I believe such a claim could have been made without running afoul of the "same damage" condition set here by the Court.

Example: Suppose workers are distressed over unsafe work conditions. We would agree the workers have a common *grievance*, even if the unsafe conditions have yet to result in any injuries, and even if each worker has a different exposure to the unsafe conditions. The workers' distress at the situation does not mean they are *equally* worried about the conditions, nor equally exposed. The workers are simply concerned about the same issue: their grievance need only be *common,* not *equal*. (See proposition two above.)

In economic terms, the Claimants similarly share a common grievance in that the risks to which they have been exposed, as a result of the alleged misconduct, are common among them (including the risk that Google misuses the data, or fails to protect it).[v]

User data can be used, innocuously enough, to deliver tailored content to users, as the Court optimistically posits. (See ruling at [8] and [9].) But that is just one reason for collecting the data, and may be only a pretext. Data can be used in a number of different ways, with many dangerous applications being commonplace.

Google is purportedly in the business of selling the data it accumulates, leaving all Claimants exposed to misconduct by Google, parties that Google contracts with, and any parties that those parties contract with, and so on. For all we know, the data might end up being "bargained for" on the dark web.

While it is unclear what Google or other parties might do with Claimants' data, apart from providing targeted advertisements,[w] Claimants are exposed to at least some of the following known risks:

- identity theft, which could result from data theft (e.g., from a hacking incident);
- telephone, mail, email, or text scams and spamming;
- unwanted, targeted advertising[x]; and

---

[v] I am not suggesting that the introduction of risk, alone, provides a basis for standing; but it may be the very definition of a "common grievance," which is at issue here in the "same interest" test. With that said, some courts have held that increased exposure to risk is sufficient to provide standing. See *Natural Res. Def. Council v. EPA*, 464 F.3d 1 (D.C. Cir. 2006) (standing based upon increased lifetime risk of developing skin cancer); *Sutton v. St. Jude Med. S.C., Inc.*, 419 F.3d 568 (6th Cir. 2005) (standing based on increased risk of harm caused by implantation of defective medical device).

[w] For example, in late 2018 the U.K. Information Commissioner's Office (ICO) fined Facebook £500,000 for serious violations of data protection law – the maximum fine allowable under the applicable laws at the time the incidents occurred. The ICO determined that "between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information without sufficiently clear and informed consent ...." According to Commissioner Denham, "Facebook failed to sufficiently protect the privacy of its users before, during and after the unlawful processing of this data." The personal information of over one million users was harvested and consequently "put at risk of further misuse." (See here.)

[x] For example, recovering addicts may not want to receive targeted advertisements tempting them to indulge in the products or behaviors from which they are recovering. (See here.)

- price discrimination[y]

If Google's alleged misconduct is taken as true, Claimants are acutely exposed to these risks:

- Google has little incentive to protect Claimants' data, because Google has no contract with them and owes them no specific obligations.
- Even if Google were motivated to protect Claimants' data, this would be difficult if Google sells the data, as Google allegedly acquired the data surreptitiously. Google would have no ownership interest in Claimants' data, and may therefore be limited in its ability to impose – and more importantly *enforce* – terms ensuring that other parties protect Claimants' data.
- According to reports, Google does not have an unblemished record for data protection.[z]

Example: The U.K. Information Commissioner's Office's investigation and ultimate fining of Leave.EU for "serious breaches of electronic marketing laws" during the 2016 Brexit referendum, demonstrates several of these risks coming to fruition. The ICO found a significant relationship (e.g., overlapping directors) to exist between Leave.EU and an insurance company Eldon Insurance Services Ltd ("Eldon"). Commissioner Denham noted that it "is deeply concerning that sensitive personal data gathered for political purposes was later used for insurance purposes and vice versa. It should never have happened."[aa] Eldon would, for example, pitch Leave.EU campaign supporters by way of email newsletters offering "10% off" for Leave.EU supporters. Leave.EU did little, if anything, to protect the acquired data when sharing it with Eldon (which trades as GoSkippy Insurance). "It was confirmed that there is no formal contract in place between Leave.EU and GoSkippy to provide direct marketing, and that the inclusion was an informal arrangement."[bb]

Acting Alone, The Individual User Is Lost

Lloyd v. Google LLC, at its core, concerns claims that Google tracked users and sold their data without their knowledge or consent – and without any contract. By the very nature of this case, if individual users sought to act alone in pursuing litigation, they would face immediate and crippling challenges:

1. Individual users would have difficulty constructing the background story for their cases, as the heart of the matter lies not in Google's conduct towards a single user but in Google's conduct towards the masses. Google is not seeking to track any specific individual, but to accumulate extensive data sets, best achieved by tracking many users.

---

[y] Price discrimination is the process of customizing prices based on a user's perceived interest or buying capacity. A wealthy consumer might be frustrated to find that information about him, such as the location of his home, is being used by companies to price online products *for him* at higher prices than those displayed to other shoppers perceived to be less wealthy. (See here and here.)

[z] When one of its databases was reportedly hacked, exposing user data, Google discovered and patched the problem without disclosing the incident to its users. (See here.)

[aa] In a similar situation, the ICO found that Emma's Diary (a website that provides pregnancy and related advice to mothers and mothers-to-be) illegally collected and sold personal information on over one million people to Experian Marketing Services, a branch of the consumer credit rating agency, "specifically for use by the Labour Party." (See here.) People's *social* information is clearly being mixed with their *financial* and *political* interests, whether they are aware of it or not.

[bb] See here and here.

2. Individual users would be at a significant informational disadvantage, given the private nature of the data market, and the secrecy of Google's own operations and contractual relationships.
3. Individuals would not have the resources or savvy to prepare and litigate this case against a well-capitalized behemoth. Additionally, the damages-per-individual would likely be negligible relative to the basic financial costs of pursuing an action, never mind the emotional cost of being in litigation or the opportunity cost of time spent.

In short, individual users would find it incredibly difficult, if not impossible, to show Google's alleged misconduct at the pleading stage of an individual lawsuit.[cc] This is where a class action is helpful: it enables under-resourced individual claimants, each with limited damages, to reach the critical mass necessary to pursue complex litigation and, if successful, prompt a change in conduct.[dd]

Closing Thoughts

Privacy concerns are not new. In 1890, revered jurist Louis Brandeis co-wrote *The Right to Privacy*, which considered, among other things, whether a person's unpublished notes, or scribbled-down thoughts, could be publicized without that person's consent.

New technologies bring with them fresh privacy concerns. With the advent of the telephone came the concern that wiretapping of telephone conversations invades the speakers' privacy.[ee] With television came the concern that filming people without permission can invade their privacy. In today's world, the Internet presents some of the most challenging privacy concerns ever faced, many of which are only now becoming apparent.

Consumers Are the Product

While the law "catches up" to define rules for appropriate conduct online, consumers are being exploited.

Large corporations (including trusted Big Tech companies) are reaping handsome rewards by selling consumers' data; but many of these companies have not done enough to protect the data acquired. Stories of data breaches, and the misuse of personal information seem to be a daily occurrence.

Consumers should be especially resentful because they do not share in the financial profits reaped from their data, but they bear the full risks of their data being compromised and misused.

[cc] It is difficult to articulate a claim, and argue for damages, when one does not know what has happened with one's data. Contracts between Google and the advertising firms are likely confidential and difficult to obtain without discovery.

[dd] A class action also solves the problem of having a potentially large number of individual claims, being lodged, that would be demanding on court systems and taxing on defendants. In late 2018, after Uber "won" key rulings from the 9th Circuit Court of Appeals in the U.S., which enabled Uber to decertify a class of 240,000 Uber drivers and preclude what would have been a class action against Uber, roughly 12,500 drivers served individual arbitration demands on Uber. (See here and here.)

[ee] It was in this context that Justice Brandeis, sitting on the U.S. Supreme Court, penned his famous dissent, in which he defined the "right to be let alone" as "the most comprehensive of rights, and the right most valued by civilized men." *Olmstead v. United States*, 277 U.S. 438 (1928). *Olmstead* considered whether the warrantless wiretapping of telephone conversations by police constituted an unlawful search and seizure. *Olmstead* has since been over-ruled, as the courts came around to the wisdom of Justice Brandeis. See, for example, *Katz v. United States*, 389 U.S. 347 (1967).

Personal Data v. Private Data

The potential for misuse of personal data brings to the fore many problems regarding the collection, storage and sale of personal data. Before these can be resolved, we need first to understand what the differences are between *personal data* and *private data*, and where the boundaries lie.

Hair color is certainly personal, but is it private given that we display it in public? What about our religious or spiritual beliefs — are they private if we practice them in public? Is the value of one's house private information? Are our thoughts and interests private, if we express them on social media? And, critically in *Lloyd v. Google*, are our online activities private?

Tracking is an Invasion of Privacy

Some exceptions notwithstanding, I believe that our online activities are private and that tracking our movements online is akin to tracking our footsteps on the roads of any city.

In the United States, the government cannot track a person's movements by installing a GPS device on the person's car, without a warrant authorizing such tracking, because this is deemed an invasion of privacy.[ff] Installing third-party cookies on someone's computer without permission, in order to track the person's online movements, is no different. In my opinion, this is an invasion of privacy.

As I have explained in this article, fixed-fee "pay-for-data" systems can easily be implemented to level the playing-field between consumers and the companies that collect their data. More complex and individualized *variable-fee* "pay-for-data" systems (algorithms) can also readily be applied.

An Analog Decision in the Digital Age

Lloyd v Google missed an opportunity to address whether tracking without permission is permissible, and also whether the data allegedly accumulated and sold by Google was *personal* or *private* data.

Additionally, the Court determined that Claimants could not proceed as a representative action – a decision which, if followed, could limit the legal remedies available to consumers

The purpose of enacting laws is to force a market correction where the market does not automatically correct itself. To combat privacy issues like those in this case, we have passed data privacy acts such as the DPA, GDPR and the California Consumer Privacy Act. These laws protect consumers. But the enacted laws have little or no bite if they cannot be effectively used to seek redress.

Richard Lloyd may have been right when he referred to the ruling as an "analog decision in digital age."

"Today's judgment is extremely disappointing and effectively leaves millions of people without any practical way to seek redress and compensation when their personal data has been misused . . . and sends a signal to the world's largest tech companies that they can continue to get away with treating our information irresponsibly."

– Richard Lloyd

* * *

[ff] See, for example, *United States v. Maynard,* 615 F.3d 544 (D.C. Cir. 2010).

PF2 Securities' research team focuses on the dynamics of financial markets and complex products. We are typically engaged in the context of dispute resolution or litigation to explain market norms from a practitioner's perspective; build or apply mathematical models and statistical techniques to analyze (potentially anomalous) market movements and patterns; and to quantify potential damages from any agreed-upon wrongdoing.

PF2 Securities has offices in New York, Los Angeles, and Sydney. For North American or European matters, email us at info@pf2se.com, or for Australian matters at info@pf2se.com.au. You can join our distribution list by signing up on the News & Research page of our website.

Disclaimer. PF2 is an independently-held consulting company. PF2 does not provide investment, legal, accounting, tax or any other advisory services. All information contained herein is protected by copyright law and may not be copied or otherwise reproduced, repackaged, transferred, redistributed or resold for any purpose, in any shape or form without PF2's prior written consent.