HEINONLINE

DATE DOWNLOADED: Thu Nov 7 06:50:05 2024
SOURCE: Content Downloaded from HeinOnline

Citations:
Please note: citations are provided as a general guideline. Users should consult their preferred citation format's style manual for proper citation formatting.

Bluebook 21st ed.
Vaclav Janecek, Data Protection, the Value of Privacy and Compensable Damage, 79 CAMBRIDGE L.J. 417 (November 2020).

ALWD 7th ed.
Vaclav Janecek, Data Protection, the Value of Privacy and Compensable Damage, 79 Cambridge L.J. 417 (2020).

APA 7th ed.
Janecek, Vaclav. (2020). Data protection, the value of privacy and compensable damage. Cambridge Law Journal, 79(3), 417-420.

Chicago 17th ed.
Vaclav Janecek, "Data Protection, the Value of Privacy and Compensable Damage," Cambridge Law Journal 79, no. 3 (November 2020): 417-420

McGill Guide 9th ed.
Vaclav Janecek, "Data Protection, the Value of Privacy and Compensable Damage" (2020) 79:3 Cambridge LJ 417.

AGLC 4th ed.
Vaclav Janecek, 'Data Protection, the Value of Privacy and Compensable Damage' (2020) 79(3) Cambridge Law Journal 417

MLA 9th ed.
Janecek, Vaclav. "Data Protection, the Value of Privacy and Compensable Damage." Cambridge Law Journal, vol. 79, no. 3, November 2020, pp. 417-420. HeinOnline.

OSCOLA 4th ed.
Vaclav Janecek, 'Data Protection, the Value of Privacy and Compensable Damage' (2020) 79 Cambridge LJ 417 Please note: citations are provided as a general guideline. Users should consult their preferred citation format's style manual for proper citation formatting.

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at https://heinonline.org/HOL/License
-- The search text of this PDF is generated from uncorrected OCR text.
-- To obtain permission to use this article beyond the scope of your license, please use: Copyright Information

he (the son) is a knowing recipient within *Williams*. So, there is no justification for preventing Mohammed Rashid from suing to vindicate his equitable interest and his claim should not be time-barred.

As if this were not enough, the case also considers the extent to which, after *Patel v Mirza* [2017] A.C. 467, "illegality" can taint a claim (i.e. Rashid's), but that is another story. For now, this case forces us to look closely at what we mean by a registered title and the extent to which it can be lost when there is a fraud. There is clearly a worry in the case that long past events should not compromise a registered title (see here the Law Commission's "long stop" proposals on rectification), but that policy goal is achieved by some imaginative, and unnecessary, intellectual gymnastics. If the aim was to confirm Rashid in his registered title after so many years, despite his complicity in fraud, there was an easier way. Under Schedule 4 to the 2002 Act, a person in possession cannot have a title rectified against them unless they have contributed to the mistake – and Rashid was knee deep in contribution. But, even then, the register need not be rectified if there are exceptional circumstances justifying a refusal to rectify. This could simply have been Rashid's long stay on the land, irrespective of whether he had adversely possessed it or not. No doubt, it is more comforting to find that Rashid has a claim of right (adverse possession), but how much simpler to just apply the LRA 2002 and exercise a discretion against rectification, not least because Mohammed Rashid may then have been entitled to an indemnity?

MARTIN DIXON

Address for Correspondence: Department of Land Economy, University of Cambridge, UK.
Email: mjd1001@cam.ac.uk

DATA PROTECTION, THE VALUE OF PRIVACY AND COMPENSABLE DAMAGE

IN *Lloyd v Google LLC* [2019] EWCA Civ 1599, [2020] Q.B. 747, the Court of Appeal adopted a broad understanding of "damage" resulting from unlawful collection of personal data, paving the way for a representative action against Google on behalf of victims of such wrongs. This could be a valuable addition to the expanding arsenal of remedies (in particular under the General Data Protection Regulation (GDPR) (Regulation (EU) No 2016/679 (OJ 2016 L 119 p.1))) against what Shoshana Zuboff has dubbed "surveillance capitalism" (see *The Age of Surveillance Capitalism* (London 2019)).

From 2011 to 2012, Google secretly tracked the Internet activity of Apple iPhone users and then used the accumulated data for various commercial purposes. This method of obtaining personal data through a web browser became known as "the Safari Workaround". Google's practice

violated the Data Protection Act 1998 (DPA), especially the duties to process the data fairly and to secure data subject's consent. Lloyd sought only damages and his claim, which proposed a tariff figure of £750 per person, was advanced also on behalf of some 4.4 million iPhone users in England. If it succeeds, Google's liability would be up to £3.3bn.

The claim was for damages that either reflect the infringement of data-protection rights, the commission of the wrong and loss of control over personal data (at [13]) or are calculated as "negotiating damages" by imagining hypothetical negotiation over their purchase (see [6], [66]–[69]). Unlike in *Vidal-Hall v Google Inc.* [2015] EWCA Civ 311, [2016] Q.B. 1003 which also concerned the Safari Workaround, no individualised harm was alleged in *Lloyd*. Indeed, Lloyd advanced the claim only in relation to generally described damage that all the represented individuals had presumably sustained, without proving any actual loss or distress, to meet the requirement of the Civil Procedure Rules 1998 (CPR) for representative actions, namely that all those represented have "the same interest in a claim" (CPR 19.6).

In light of the principles governing permission to serve proceedings outside the jurisdiction (CPR 6.37), the court had to decide whether the facts alleged amount to "damage" pursuant to DPA, s. 13 which entitles any "individual who suffers damage by reason of any contravention ... of the requirements of this Act" to compensation.

At first instance, Warby J. ([2018] EWHC 2599 (Q.B.), [2019] 1 W.L.R. 1265) held that the wording of section 13 requires proof of both the DPA contravention and consequential damage because some contraventions of the DPA would not result in damage. In his view, while the underlying wrong amounts to loss of the right to control the use personal data, "loss of control" over data cannot constitute the damage in question because it does not "result from" the wrong – it is the wrong (at [58]). Since no consequential damage was alleged, the judge concluded that the pleaded facts did not disclose any basis for claiming compensation.

In addition, Warby J. held that even if there was "damage" for section 13, the members of the class of iPhone users did not suffer the same damage and thus did not have the "same interest" in the claim. Given the (imagined) different levels of Internet use, the impact the Safari Workaround "will have varied greatly" (at [90]). He therefore refused permission to serve proceedings on Google. Lloyd appealed.

Allowing the appeal, Sir Geoffrey Vos C. (Davis L.J. and Dame Victoria Sharp P. concurred) held that a claimant can recover damages for loss of control of their data under DPA, s. 13, without proving pecuniary loss or distress, and that the members of the class that Lloyd sought to represent did have the same interest (at [88]).

Sir Geoffrey Vos C. agreed with Warby J. that section 13 requires proof of both a contravention and consequent damage. However, unlike Warby J., he concluded that "loss of control" falls within the remit of damage. Indeed,

for the Court of Appeal "loss of control or loss of autonomy over their personal data" was critical to the characterisation of the class members' loss (at [45]). Sir Geoffrey Vos C. saw loss of control as "damage" for two reasons. The first was one of logic. Given that control over data is in fact a tradeable asset, it must have an economic value and loss of this asset must therefore amount to "damage" pursuant to DPA, s. 13 (at [46] and [47]). The second was based on analogical application of the Court of Appeal's ruling in *Gulati v MGN Ltd.* [2015] EWCA Civ 1291, [2017] Q.B. 149 – a case of misuse of personal information (MPI) where the claimants obtained compensation for "loss of control" in the context of large-scale phone hacking. Sir Geoffrey Vos C. relied on the analogy (at [48]–[57]) because both MPI and DPA torts protect the right to privacy; it would be wrong in principle to protect that right by "loss of control" damages in the MPI context but not in the DPA context; and "the EU law principles of equivalence and effectiveness point to the same approach being adopted to the legal definition of damage in the two torts" (at [57]). Additionally, he felt that his conclusion was supported by Recital 85 of the GDPR that specifically mentions "loss of control over personal data" as an example of damage.

These two accounts of how the claimants suffer "damage" must be recognised as distinct. Not all "personal data" (and not all personal data that has "value") is protected by the action for "misuse of private information". The first account given by the Court of Appeal turns on the value of accumulated data and is justified primarily by the "personal" dimension of accumulated data, while the second account it is derived from its "private" dimension. Misuse of private information depends on the existence of a "reasonable expectation of privacy" which must be, by its very nature, individualised. There is no such thing as reasonable expectation of privacy in relation to all personal data of any individual, let alone in relation to the data of a whole class of iPhone users. Some personal information acquired by Google was surely public. Besides, because Google can profit from the unlawfully obtained data does not mean that each data subject suffers harm. The supposed symmetry is illusory. While the idea of an unjust profit could in principle justify a restitutionary remedy such remedy cannot be found in DPA, s. 13.

Interestingly, the Court of Appeal and High Court seem to have reached different conclusions mainly because they were focusing on different facts (although they both referred to "loss of control over personal data" in their reasoning). This was because both courts analysed the meanings of "damage" and "loss of control over personal data" merely as abstract questions of law since Lloyd did not seek to "allege or prove any distinctive facts" (at [3]). However, "loss of control over personal data" is an ambiguous notion. The phrase has at least three distinct meanings: (1) loss of a right to control the use of personal data; (2) loss of digital data that are reasonably likely to reveal personal information (e.g. data about Internet usage

may sometimes be seen as personal data); or (3) misuse of personal and formerly private information (e.g. if one Googles "abortion" and wants to keep this information private). This ambiguity springs from how, on a factual level, the categories of data, personal data, and personal and private information relate to each other. Unfortunately, it is hard to tell which of the three meanings the courts had in mind. Warby J. probably used the first meaning, while Sir Geoffrey Vos C. vacillated between the second and the third. GDPR Recital 85 offers no further clarity, relating as it does to an entirely different matter.

The Supreme Court has granted leave to appeal. The decision will be important not just for the litigants but also for all those who compete for our data and attention in the digital economy as well as for those who guard our freedom against these omnipresent practices. Importantly, the concept of damage pursuant to DPA, s. 13 overlaps with damage as defined by the Data Protection Act 2018 (s. 169) and the GDPR (art. 82), which is why it would be helpful if the Supreme Court decides which of these accounts of damage (if either) is relevant, and keeps them distinct. Further, if the Supreme Court will consider whether an award for this damage can be assessed as "negotiating damages" (Warby J. rejected this, but Sir Geoffrey Vos C. thought it not unarguable), it should be kept in mind that the right to consent with the processing of personal data, namely the "private" dimension of data, cannot be waived (GDPR, art. 7(3)). If loss of control over this dimension is non-waivable, can the courts imagine any legitimate negotiation over such assets? Online platforms as well as those of us who click "I agree" several times a day deserve more clarity on this point.

VÁCLAV JANEČEK

Address for Correspondence: Faculty of Law, University of Oxford, Oxford, OX1 3UL, UK.
Email: vaclav.janecek@law.ox.ac.uk

BEAR RAIDS AND MARKET MANIPULATION: MUDDYING THE WATERS?

ARTICLE 15 of the Market Abuse Regulation (Regulation (EU) No 596/2014 (OJ 2014 L 173 p.1)) (MAR) states that "a person shall not engage in or attempt to engage in market manipulation". In accordance with Article 16 of the MAR, prevention and detection of such manipulation on the London markets is a matter for the London Stock Exchange (LSE) and Financial Conduct Authority (FCA) (Financial Services and Markets Act 2000 (as amended) (FSMA) and Financial Securities and Markets Act 2000 (Market Abuse) Regulations, SI 2016/689, r. 3). In *Burford Capital Limited v London Stock Exchange Group plc.* [2020] EWHC 1183 (Comm), Andrew Baker J. was asked to consider whether