Editors: Deven McGraw, dmcgraw@manatt.com | Katrine Evans, katrine.evans@privacy.org.nz

Vidal-Hall and Risk Management for Privacy Breaches

Katrine Evans | Hayman Lawyers

The March 2015 decision of the English Court of Appeal case Google v. Vidal-Hall increases customers' ability to sue for misuse of private information, updates definitions of personal data, and allows for consumer compensation for emotional distress without accompanying financial loss.[1] If the decision survives the appeal to the UK Supreme Court, many Internet-based businesses—including those outside the UK—will need to adjust their risk management practices for privacy breaches. (The Supreme Court agreed to hear the appeal on 28 July 2015.)

In this article, I argue that the Vidal-Hall decision supports the policy of privacy law, particularly data protection legislation. The case provides some of the most compelling incentives for investment in data protection that we've seen in many years.

Risk Management and Privacy Breaches

In a globally networked world, a business decision to design a product or service that turns out to breach privacy can end up being eye-wateringly expensive. The same is true for a failure to keep information properly secure.

Popular businesses collect and use the personal information of thousands—even millions—of individuals, often across different jurisdictions. What happens if these people suffer harm as a result of a data breach or as a consequence of deliberate business choices? If a business must pay compensation, its bill will become very big, very quickly—even without the costs related to diagnosing the problem or repairing systems. Determining the risks of harm to individuals needs to factor large in risk planning.

Calculating this risk isn't easy. However, if people can claim compensation only when they've suffered financial loss, business risks are relatively limited. Financial loss caused by privacy breaches is far less common than distress—that is, humiliation, embarrassment, or injury to feelings.[2] It's also more quantifiable, less subjective, and more predictable.

In some countries, data protection laws let claimants sue for compensation for distress even in the absence of any financial loss. New Zealand is one example; the European data protection directive also anticipates recovery of damages for distress. However, until March, UK data protection legislation did not let claimants receive compensation for distress unless the breach had also caused financial loss. The landmark English appeal decision of Google v. Vidal-Hall changed all that. Unless the UK Supreme Court overturns the decision, compensation for distress alone will be available under the Data Protection Act (DPA).

In Google v. Vidal-Hall, the Court also indicated that "personal data" is a broader category than businesses might have anticipated. In addition, the Court confirmed that it's possible to serve businesses overseas with proceedings for misuse of private information and breach of the DPA.

Agencies subject to English law might need to revise their risk calculations by investing more in effective accountability and privacy breach prevention and developing good strategies to assist their customers when mistakes occur and their privacy is compromised (for example, in data breach situations). Such change won't be cheap. However, the alternative—waiting until disaster strikes—could be ruinous.

Google v. Vidal-Hall

The Vidal-Hall grievance stemmed from Google's placement of a cookie on devices using Safari. The cookie let Google collect browser-generated information that was fed

Copublished by the IEEE Computer and Reliability Societies

to its DoubleClick service, which delivered advertising to consumers based on their online behavior and ostensible preferences. Because Google had stated that it would not collect information from Safari users without express consent, this "Safari workaround" landed Google in hot water with regulators in the US, leading to a settlement with the US Federal Trade Commission for US$22.5 million and other major settlements with other US states.[3] Regulatory intervention such as this is valuable as it can require agencies to bring their practices in line with the law, but it does not provide a right of redress for the consumers themselves. However, bringing claims in civil court is not easy. Financial loss from these types of collections and uses of information is relatively uncommon, and emotional harm is often negligible or hard to prove.

Despite the difficulties, three individual claimants filed proceedings in the English courts against Google for misusing their private information with the Safari workaround, and for breaching the DPA. They sought damages for distress, acknowledging that they had not suffered financial loss.

The case finally reached the Court of Appeal. The issue was a technical one: Could the claimants serve Google in California with proceedings in an English court? The Court of Appeal considered the strict rules for offshore service and decided that, in this case, the proceedings could go ahead. The individuals persuaded the judges that their claim had a serious chance of succeeding. All three major aspects of the claim—misuse of private information, the definition of personal data, and compensation for distress—have repercussions for agencies that deal with personal data, particularly online.

Misuse of Private Information

For historical reasons, English law distinguishes between actions in tort (a recognized and structured form of civil wrong) and actions in equity (a more flexible request to the court to exercise its sense of fairness to redress a situation). Damages were available in tort; injunctions, for instance, come from equity. The distinction is usually immaterial in practice—the main courts can hear any kind of claim and can award whatever remedies are required. However, the rules relevant to the Vidal-Hall case state that respondents located offshore can only be served with proceedings in tort. If the claim is in equity, service won't be allowed and the offshore company won't have to face a claim in the English courts.

Vidal-Hall provides a good testing ground for determining where the boundaries of personal data lie in English law.

Google probably thought it was on fairly safe ground here. Unlike US law, English law has a long tradition of denying the existence of a standalone privacy tort.[4,5] Instead, it has addressed privacy claims by extending the equitable action for breach of confidence. So, for instance, kiss-and-tell stories about footballers' extramarital affairs, celebrities seeking medical assistance for addiction, photographs of celebrity children, and phone-hacking practices have all featured in breach of confidence cases in the past 15 years.

However, more recently, the courts have increasingly recognized that breach of confidence differs from misuse of private information. Breach of confidence is easy to identify when it imposes a duty not to disclose secret information that was imparted in a relationship of trust (for instance, in doctor/patient or trade secret situations). It is relatively narrow, focused, and clear. However, most new privacy cases do not involve relationships of trust. Instead, the affront is to autonomy and dignity. Extending breach of confidence to fit privacy claims can lead to confusion and strained reasoning—implying expectations and relationships where none exist in reality. It has worked but only because the courts have been determined to make it work and because European law demands that privacy be properly recognized.

The Court of Appeal in Vidal-Hall has abandoned artificiality and confirmed that misuse of private information is a tort in English law.[1] It said that it wasn't creating a new tort but simply describing the existing law. However, this downplays the decision's impact. Stating that there's a tort of misuse of private information is groundbreaking. It releases privacy from the limitations imposed by confidentiality and will almost certainly extend the range of privacy issues that the courts can consider (for instance, situations in which businesses use information that isn't published to third parties). As the Google situation demonstrates, it also heightens the chances that offshore businesses using the personal information of people in the UK can be sued in the UK.

The Supreme Court has confirmed that the tort exists and refused to hear Google's appeal on that point. So it will be worth watching carefully to see how the court at the substantive hearing defines "private information" for tort. Based on UK court cases so far, the courts might limit the tort to situations in which use of the information would be highly offensive to a reasonable person,

or in which there are "reasonable expectations of privacy." Whether tracking online activity and targeting advertising breach reasonable expectations of privacy will be an interesting debate.

Personal Data

As it happens, the definition of "misuse of private information" might matter less in this case than in others because the Court also decided that there was a separate basis for the proceedings under the DPA. The DPA is triggered in cases involving "personal data"—data about a living individual who can be identified either from the data itself or from the data and other information in the possession of, or likely to come into the possession of, the data controller.

The data doesn't have to be particularly sensitive. Claimants don't have to show that they have a reasonable expectation of privacy. If the activity breaches one of the data protection principles, that's enough.

As a result, the Court had to consider whether it was seriously arguable that browser-generated information was personal data, and it decided that it was. Relying on European expert views and law, the Court said that identifiability hinges on a person's distinguishability from other members of a group. It doesn't matter that a person's name isn't attached to the information.

Factors that made it arguable that the data in question was "personal data" included the following:

- The DoubleClick cookie ascribed a unique ID code to the device, allowing tracking of websites visited, times visited, time spent on the website, and so on.
- In this era of the smartphone and tablet, devices are generally used exclusively by a single user. Identifying the device therefore identifies the user.
- The browsing habits of real individuals—not just devices—are being recognized and tracked.
- Google's business model was based on its ability to individuate users and target advertising based on their interests.
- The fact that the data controller might not actually use the information to identify an individual is immaterial. The question is whether they can do so if they wished (for example, linking an IP address to a Google account).
- Targeted advertising reveals information about a user's browsing history. A notional third party with access to the device could therefore discover information about the user. Whether this is enough to make Google liable for the processing of personal data is arguable, but the Court wasn't prepared to dismiss the possibility.

The question of what amounts to personal data is an important one for businesses. The debate will continue at both a legal and technical level for a long time to come. However, Vidal-Hall provides a good testing ground for determining where the boundaries of personal data lie in English law. If browser-generated information is personal data, other things might be as well—for example, the new trend for companies to identify other apps that are loaded on a device that uses their product, and profile the user accordingly. Businesses looking for new ways to monetize what they do by profiling users will have to pay particular attention to data protection requirements.

Compensation for Distress

The issue that has attracted most comment is the claim for compensation for distress. The DPA deliberately excludes claims for compensation for distress unless there's also pecuniary or other material loss. Section 13 is unequivocal:

> (1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.
>
> (2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller if–
>
> (a) the individual also suffers damage by reason of the contravention, or
>
> (b) the contravention relates to the processing of personal data for the special purposes [defined in section 3 and not relevant here].

The Act draws a clear distinction between damage (pecuniary loss) and distress (emotional harm).

This is at odds with European law, which allows for recovery of compensation for distress alone. The Court decided that it wasn't possible to interpret section 13(2) in a way that would align with European law; the two were incompatible.

In addition, the Court had to consider article 47 of the European Union Charter of Fundamental Rights, which states that everyone has the right to an effective remedy if the rights and freedoms guaranteed by EU law are violated. Established case law says that domestic courts must disapply the conflicting provision, unless this would require the Court to redesign the fabric of the legislative scheme.[6]

The Court found that it could disapply section 13(2) without redesigning the DPA's scheme. Section 13(1) would still stand, and "damage" would refer to harm of any kind—both pecuniary loss and distress. As a result, unless the

Supreme Court reverses the decision, the limitation on compensation in section 13(2) of the DPA is dead. Claimants can now sue in the UK for distress alone.

Whether the claimants had in fact suffered emotional distress is still up in the air. That will be an issue for the trial court to consider. However, the claimants provided some information confidentially to the Court of Appeal that was sufficient to persuade the judges that their claim for emotional distress was plausible. The court acknowledged that compensation would be modest, but "the issues of principle are large."[1]

The Decision Strengthens Data Protection Regulation

To some extent, the risk of having to pay compensation for distress without any financial loss already existed. From what the Court says in Vidal-Hall, the section 13(2) restriction was often artificial. Claimants could identify a nominal financial loss and then claim compensation for the real harm (the distress). The Court cited the 2013 case of Halliday v. Creation Consumer Finance wherein the nominal financial damage was £1, but the defendant conceded that the Court could then give distress compensation (£750). Other courts have followed this example. A determined and well-advised litigant could therefore easily circumvent the restriction.

As a result, many businesses should already have evaluated the risk of paying compensation for distress. However, the Court's decision brings new focus to those risk calculations. In addition, there's a heightened possibility that—at least for a time—claimants will take their cue from Vidal-Hall and be more willing to sue.

Aside from the issue of targeted online advertising, Vidal-Hall's most noticeable impact might be on risk management for data breaches. Many data breaches don't result in financial loss, but distress is common. For instance, a breach involving sensitive health information is more likely to cause anxiety and damage trust than financial loss. Because data breaches often involve large numbers of people, the potential cost of managing distress claims is a major addition to the costs inherent in data breach situations.

Agencies' best defense against the risk is to pay more attention to their privacy practices and improve their standards of protection.

Agencies' best defense against the risk is to pay more attention to their privacy practices and improve their standards of protection. Areas to focus on include

- building a secure system that doesn't violate data use laws;
- ensuring that staff and other system users do not circumvent the privacy protections that have been set up;
- looking beyond legal compliance and focusing on preventing mistakes—for instance, investing in system improvements and engaging principles of privacy by design (investing in good design will also reduce the risk of costly system fixes later); and
- responding to customers quickly and fairly when problems do arise to address any real distress or harm that is caused.

Not all businesses will have to redesign their data management practices. Responsible businesses don't operate with a cavalier disregard for whether they cause their customers distress. Every business owner knows that reputation is vital for success and efficiency and that customer attitudes directly impact the bottom line. Many will already have invested in sound data management. So, although the legal change is very significant, the impact on many businesses' systems might not be dramatic.

However, to the extent that some agencies will have to improve their privacy practices, this ruling is a positive change that supports data protection policy. The law requires agencies to treat personal data with care, but there are fewer incentives to comply if agencies must only account for breaches that cause financial loss. The decision is also right in principle. Permitting compensation for distress recognizes the real harm that individuals can suffer when their information is misused or leaked in breach of the law.

Of course, the Vidal-Hall decision appears to open the door for large numbers of claimants to bring relatively trivial distress claims. However, the experience of jurisdictions in which such claims are already technically possible suggests that the courts will gradually develop boundaries to deter less meritorious claims.

Questions we must ask about the viability of distress claims include the following:

- How serious must the distress be before someone can file a claim? Will seriousness of distress determine the amount of compensation?
- Will the courts be more likely to reject claims for low-level distress on the grounds that the claim is vexatious, raises trivial matters, or is an abuse of process?
- What level of formal evidence will the courts require to prove distress?

- How strict will the courts be about causation—that is, does the distress need to flow from the privacy breach? Must the breach be the sole cause of the distress, or only one cause?
- How large will the awards for distress be? (Given the time, stress, and money required to go to court, this might be as much—or perhaps more—of an incentive for litigation than the technical availability of compensation).

It's in agencies' interests to limit their exposure to risk, and it's therefore unsurprising that Vidal-Hall's conclusions are controversial. However, if the UK Supreme Court upholds the Court of Appeal's decision, the net effect will likely be improved privacy protection for individuals in many areas of their lives, including online. ■

References

1. Google v. Vidal-Hall and others, EWCA (England and Wales Court of Appeal, Civ 311, 2015.
2. "Damages Awarded under the Privacy Act 1994–2011," Human Rights Review Tribunal, Ministry of Justice; www.justice.govt.nz/tribunals/human-rights-review-tribunal/decisions-of-the-human-rights-review-tribunal/damages-awarded-under-the-privacy-act.
3. "Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser," Federal Trade Commission, 9 Aug. 2012; https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.
4. Kaye v. Robertson, FSR (Fleet Street Reports) 62, 1991.
5. Wainwright v. Home Office, 2 AC (Appeals Cases) 406, 2004.
6. Benkharbouche and Janah v. Embassy of Sudan and others, EWCA, Civ 33, 2015.

Katrine Evans is a senior associate at Hayman Lawyers, Wellington, New Zealand. Contact her at k.evans@haymanlawyers.co.nz.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.