Liability and remedies for data protection and privacy infringements

Dr. Zoi Krokida

zoi.krokida@stir.ac.uk

Overview

- Primary liability: controllers and processors
- Secondary liability: employers, representatives, directors
- Private enforcement: individual remedies and class actions
- Public enforcement: investigative and corrective powers
- Privacy infringements: remedies

Liability for data protection violations

- **Data controller** (Art. 4(7)) - the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing** of personal data
- **Data processor** (Art. 4(8)) - a natural or legal person, public authority, agency or other body which processes personal data **on behalf** of the controller
- **Obligations** under the UK GDPR **will vary** depending on whether you are a controller, joint controller or processor
- The ICO has the power to take **action against controllers and processors** under the UK GDPR
- Individuals can bring claims for **compensation** against both controllers and processors

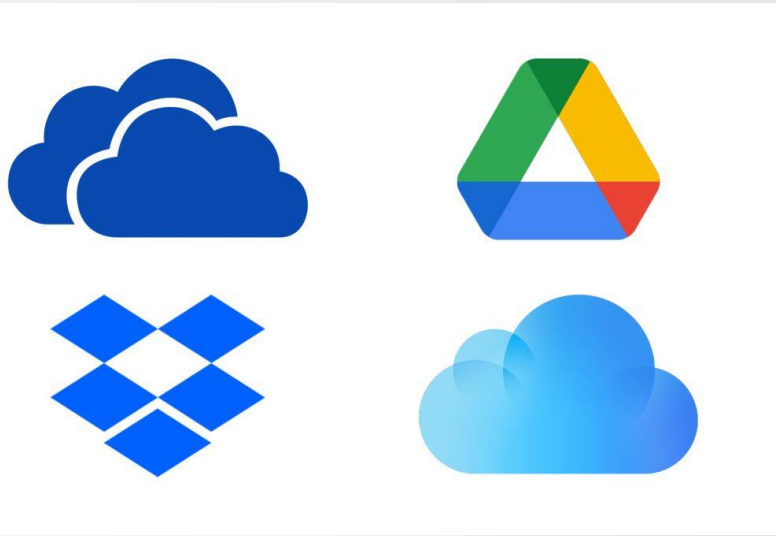
- The UK's spy agencies have given a contract to Amazon Web Services (AWS) to host classified material in a deal aimed at boosting the use of data analytics and artificial intelligence (AI) for espionage, the Financial Times reported.
- Britain's GCHQ spy agency championed the procurement of a high-security cloud system and it will be used by sister services MI5 and MI6, as well as other government departments such as the Ministry of Defence during joint operations, the report added.

Amazon strikes deal with UK spy agencies to host top-secret material

Controllers' obligations

- Comply with, and demonstrate compliance with, all the data protection principles as well as the other UK GDPR requirements
- Notifying personal data breaches to the ICO unless unlikely to result in a risk to the rights and freedoms of individuals (within 72h)
  - Notifying affected individuals (if the breach is likely to result in a high risk to their rights and freedoms)
- Also responsible for the compliance of the relevant processor(s).
- Pay the data protection fee

Processors' obligations



- Direct obligations of processors under the UK GDPR:
  - Process on instructions from a controller
  - Enter into binding contract with controller
  - Appropriate tech and organisational security measures
  - Notify the controller of any data breach without undue delay
  - Notify also Data Protection infringements
  - Accountability (maintaining records and appointing a data protection officer)
  - International transfers
  - Co-operation with supervisory authorities

Data controller – specific UK rules

- If a law ('**enactment**') imposes the obligation to process data and determines the purposes and means of processing, that law decides who is the controller (DPA, s 6(2))
- If person acting on behalf of the **Crown** determines purposes and means, the controller is…
  - Royal Household, the Keeper of the Privy Purse
  - Duchy of Lancaster, such person as the Chancellor of the Duchy appoints
  - Duchy of Cornwall, such person as the Duke of Cornwall appoints (s 209)
- On behalf the HoC, Corporate Officer of that House (s 210)

Joint controllership

- Two or more controllers **jointly determine the purposes and means** of processing, and the data subject may exercise their **rights against each** of them (UK GDPR, art 26)
- **Transparent arrangement**: joint controllers shall in 'a transparent manner determine their respective responsibilities for compliance with the obligations' (art 26(1))

Wirtschaftsakademie Schleswig-Holstein (2018)

- The CJEU held that **Facebook and the administrators of fan pages** hosted on that platform were jointly responsible for the processing of the personal data of the fan page's users.
  - The administrator of a fan page, by creating the page, (1) 'gives Facebook the opportunity to place **cookies** on the computer or other device of a person visiting its fan page' [35] and (2) influences the processing by defining 'the criteria in accordance with which the **statistics** are to be drawn up and even designat(ing) the categories of persons whose personal data is to be made use of by Facebook' [36]

Employees?

- Employees of the controller are **not processors**
- ICO: as long as they are acting **within the scope of their duties** as an employee, they are acting as an **agent of the controller** itself. They are part of the controller, not a separate party contracted to process data on the controller's behalf.

Can employers be vicariously liable for data breaches committed by their employees?

- The key authority is *WM Morrisons Supermarkets plc (Appellant) v Various Claimants (Respondent)* [2020] UKSC 12 ('*Morrisons 2*')

Vicarious liability

- In common law an employer is vicariously liable for the ***tortious* acts** (e.g. negligence) of its employees if they are carried out "**in the course of employment".**
- Common law principle of **strict**, no-fault liability for wrongs committed by another person; a form of secondary liability.
- As Lord Sumption JSC put it in *Bilta (UK) Ltd v Nazir (No 2)* [2015] UKSC 23:
  - "extends far more widely than responsibility under the law of agency: to all acts done within the course of the agent's employment, **however humble and remote** he may be from the decision-making process, and even if his acts are **unknown** to the principal, **unauthorised** by him and adverse to his interest or **contrary to his express instructions** (*Lloyd v Grace Smith & Co* [1912] AC 716), indeed even if they are **criminal** (*Lister v Hesley Hall Ltd* [2001] UKHL 22)" [70]

Vicarious liability - rationale

The imposition of liability on a no-fault basis is policy driven (*Majrowski v Guy's and St Thomas's NHS Trust* [2006] UKHL 34)

Key considerations are that:

- **Economic activity** carries a **risk of harm to others**. Fairness requires that those responsible for this activity should be liable to anyone suffering loss from wrongs committed in the conduct of the enterprise.
- Imposing strict liability on employers encourages them to maintain **standards of good practice** by their employees.

Vicarious liability – the test

1. Is it a **relationship** to which vicarious liability applies?
   - Employment but also relationships akin to it e.g. partnerships (five factors in *Various Claimants v Institute of the Brothers of the Christian Schools* [2012] UKSC 56)
2. Is the **primary wrongdoer in breach of a relevant duty**?
   - Common law torts (*Majrowski*)
   - Breaches of statutory obligations (*Morrisons 2*)
3. Is there a **sufficient connection**?
   - Sufficient connection **between the wrongs and the employee's employment** such that it would be fair to hold the employer to be vicariously liable

Sufficient connection

3. Is the wrongful conduct so closely connected with the acts the primary wrongdoer was authorised to do (or the role or "field of activities" entrusted to the wrongdoer) that, for the purposes of the liability of the employer, it may fairly and properly be regarded as done by the employee while acting in the ordinary course of its employment?

3.1. Identification of the **nature of the wrongdoer's job or field of activities** (as it was put in *Mohamud v WM Morrison Supermarkets plc* [2016] UKSC 11 [44]), or what the employee was **authorised to do** (the preferred formulation in *Morrison 2*), and

3.2. Evaluation of whether this is a sufficient connection

Morrisons 2 - facts

- This appeal concerns the circumstances in which an employer is vicariously liable for wrongs committed by its employees, and also whether vicarious liability may arise for breaches by an employee of duties imposed by the Data Protection Act 1998 ("DPA 1998").
- Andrew Skelton, one of the supermarket chain's employees (internal audit team), had been **tasked with transmitting payroll data** for the appellant's entire workforce to its external auditors
- He reacted to **disciplinary proceedings** by uploading payroll data of 100.000 employees on a **filesharing website** and sending it to 3 **newspapers**
- A newspaper notified **Morrisons** which **immediately took steps** to remove the data and links to the website.
- S was convicted of offences under the Computer Misuse Act 1990 & DPA.
- **The issue was whether Morrisons was liable, directly or vicariously, for S's actions.**

Morrisons 2 - facts

- In a **class action**, 5518 affected employees claimed **compensation** from Morrisons for breach of statutory duty under the DPA, misuse of private information, and breach of confidence against Morrisons for its vicarious liability for Skelton's acts. Skelton had already been prosecuted but the fellow employees had an interest to go after the employer: a) because of its **deeper pockets** (higher damages), b) whereas a data controller's statutory liability under the DPA is based on a lack of reasonable care, vicarious liability for an employee's conduct requires **no proof of fault**.
- **At trial**, the judge concluded that the appellant bore no primary responsibility but was **vicariously liable on each basis claimed.**
- The Supreme Court allowed the appeal.

Morrisons 2 – (a) Field of activity

- Employers can be held vicariously liable only if the 'close connection' test is met (*Mohamud*; *Dubai Aluminium Co Ltd v Salaam* [2003] 2 AC 366).

- '**Close connection**' means that the wrongful conduct was so closely connected with acts the employee was **authorised to do** that for the purposes of the liability of the employer to third parties, that it may fairly and properly be regarded as done by the employee while acting in the ordinary course of his employment.

Close connection

- The first question to ascertain 'close connection' is what functions or '**field of activities**' the employer had entrusted to the employee.
- The Court of Appel misunderstood this question and it mistakenly held that the online disclosure of the data was part of Skelton's "field of activities".
- The Supreme Court overturns this as it was not an act which Skelton **was authorised to do**: "Skelton was not engaged in **furthering his employer's business** when he committed the wrongdoing in question. On the contrary, he was pursuing a **personal vendetta**, seeking vengeance for the disciplinary proceedings some months earlier" [47]

Morrisons – (b) Sufficient connection

- The second question of the 'close connection' test is whether there was **sufficient connection between the position** in which the worker was employed **and the wrongful conduct** to make it right for the employer to be held liable under the principle of social justice.
- Unlike the Court Appeal, the Supreme Court held that a **temporal or causal connection alone does not satisfy** the close connection test and that **motive is a crucial factor** to assess (whether he was acting on his employer's business or for purely personal reasons was highly material)
  - **The fact that Skelton was acting for purely personal reasons rather than on his employer's business indicated that there wasn't a close connection between the data breach and the position in which he was employed.**

Liability of representatives

- Controllers and processors **established outside the EU must designate a representative in the EU** if the EU GDPR applies i.e. UK business offering goods/services to individuals in the EEA or monitor their behaviour.
  - Unless public authority or occasional processing of low risk
- Representatives **"to be addressed in addition to or instead of the controller or the processor** by, in particular, supervisory authorities and data subjects, **on all issues related to processing, for the purposes of ensuring compliance** with" the GDPR (art 27)
- *Rondon v Lexisnexis Risk Solutions UK Ltd* [2021] EWHC 1427 (QB) UK compliance business which represented a US company (WorldCo) in its business of supporting compliance with money laundering laws. WorldCo's database contained profiles of individuals, including the claimant's.

- Is the representative personally liable for the controller's actions in the processing of data?

Is the representative personally liable for the controller's actions in the processing of data? No

- Reps have **directly-imposed functions** i.e. record keeping, providing local transparency and availability to data subjects together with local regulatory co-operation: **they are not controllers/processors as no power on a day-to-day basis over how and why data were processed → a limited role**
- EDPB Guidelines **not law, but weight beyond expert commentary** on the text: **rep "not itself responsible for complying with data subject rights" (ibid 27)**
- Recital 80: **rep "should be subject to enforcement proceedings in the event of non-compliance by the controller or processor"** – not possible to "use a recital to cantilever into the operative text an entire system of liability for which it has not, or not sufficiently, visibly provided" (*Rondon* [98]) → representative liability is a policy tide which receded and rec. 80 is its watermark → interpreted as "subject to the possibility for supervisory authorities to initiate enforcement proceedings **through** the representative" [100]

Civil remedies (individual)

- If any of the principles, rights, and obligations are not complied with, there are remedies
- Right to lodge a complaint with a **supervisory authority** (Art. 77) - in the UK, the ICO
- Right to an **effective judicial remedy** against a supervisory authority, a controller or a processor (Art. 78-79)
  - Compensation (Art. 82)
- Right to mandate a **not-for-profit body** to represent (Art. 80)

Non-pecuniary loss

S. 13 (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 for that distress 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.

- *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 Google had secretly tracked private information about the users' internet usage via the use of cookies without their knowledge or consent and given the information to third parties
- On a **literal interpretation**, the users were not entitled to recover damages under s.13 DPA 1998 because their claims did not fall within either s.13(2)(a) or s.13(2)(b) (compensation for **(a) damage; or (b) damage and distress** - but not, generally, distress alone)

Non-pecuniary loss

- **Although there was nothing to suggest that the DP Directive required compensation for such damages to be paid, the natural and wide meaning of "damage" in art 23 included "moral", non-pecuniary damage, such as distress, *Leitner v TUI Deutschland GmbH & Co KG* [2002] E.C.R. I-2631 applied**
  - "In reaching this conclusion, we have regard to the **aim of the Directive** [76] "Since what the Directive purports to protect is privacy rather than economic rights, it would be strange if the Directive could not compensate those individuals whose data privacy had been invaded by a data controller so as to cause them emotional distress" [77]
  - "it is **irrational** to treat EU data protection law as permitting a more restrictive approach to the recovery of damages than is available under article 8 of the Convention (…) which is recognized both in article 8 of the [Convention] and in the general principles of Community law". The enforcement of privacy rights under article 8 of the Convention has always permitted recovery of non-pecuniary loss" [77]
  - Charter made specific provision for the protection of personal data: "It would be strange if that fundamental right could be breached with relative impunity by a data controller, save in those rare cases where the data subject had suffered pecuniary loss as a result of the breach. It is most unlikely that the Member States **intended** such a result" [78]

Compensation for distress due to inaccurate data (*Aven v Orbis Business Intelligence Ltd* [2020] EWHC 1812 (QB))

- An intelligence services company, had been commissioned by persons within the US Democratic Party to provide intelligence concerning any links between Putin and Trump.
- Complaints alleged that the report included personal data relating to them; that, contrary to the fourth data protection principle, the data were **inaccurate**; and that, contrary to the first data protection principle, the defendant had processed the data **unfairly or unlawfully**. They sought rectification, blocking, erasure and destruction, and a declaration that the data were inaccurate.

Lawfulness, fairness and transparency.
Purpose limitation.
Data minimisation.
Accuracy.
Storage limitation.
Integrity and confidentiality (security)
Accountability.

Aven v Orbis Business Intelligence - issues

- The issues were whether-

(1) the report contained **personal data**;

(2) the defendant's processing of the data was protected by the **national security exemption** in s.28(1);

(3) the defendant processed the data in breach of the **first or fourth data protection principles**.

Aven v Orbis Business Intelligence – personal data

- The court had to take a **holistic approach** to determining whether information contained personal data. It had to view the report as a whole, rather than adopting an item-by-item approach (*NT1 v Google LLC* [2018] EWHC 799)
- Identified the Claimants as giving significant favours to, and receiving them from, President Putin. That information was personal data: it **focused on the Cs**, was **biographically significant** and **impinged on their privacy** in a business context.
- Asserted that the Claimants used a third party to deliver "illicit cash" to President Putin. The implication of criminality made that information "**sensitive** personal data".

Aven v Orbis Business Intelligence - Accuracy

- Disclosures were lawful because for **national security** and to fulfil **contractual obligations** – **no violation of 1st** DP principle.
- Allegation concerning the illicit cash delivery was inaccurate, and although D had **accurately recorded what it was told** by its sources, it had **not taken reasonable steps to verify** that allegation, *Hussain v Sandwell Metropolitan BC* [2017] EWHC 1641 (Admin) applied.

Aven v Orbis Business Intelligence - Accuracy

- Pursuant to s.13, DPA, Messrs Aven and Fridman were entitled to compensation for any damage suffered by the defendant's disclosure of the "illicit cash" allegation. "Damage" was not confined to material loss: compensation could be awarded for distress and interference with the data subject's control over their data. The Judge also held, albeit cautiously, that where the inaccurate information was seriously defamatory, compensation could be awarded for reputational harm. Applying established defamation law principles on the assessment and mitigation of damages, as set out in Barron v Vines [2016] EWHC 1226 and Sloutsker v Romanova [2015] EWHC 2053 (QB), Warby J awarded the first and second claimants £18,000 each.

Class action for loss of control

- *Lloyd v Google LLC* [2019] EWCA Civ 1599 - appellant represented 4 million iPhone users in an action seeking damages for breach of statutory duty against the respondent for allegedly tracking their internet usage (browser-generated information) during a certain period for commercial purposes
- Queen's Bench refused the appellant's application for permission to **serve the proceedings on the respondent out of the jurisdiction** on the basis that:

(1) none of the represented class had suffered damage

(2) Members of the class did not have the same interest within CPR rule 19.6(1) so as to justify the claim proceeding as a class action ('representative' action)

However……

- **Court of Appeal**: damages were capable of being awarded for **loss of control** of data under the DPA 1998, s 13 (compensation), **without proving pecuniary loss or distress**. A representative action against Google for damages for alleged use of browser-generated information without consent was allowed to proceed.

Lloyd v Google – damage

- In providing that an "individual who suffered **damage by reason of any contravention**" was entitled to compensation, s.13 was **implementing DP Directive art 23**
- Language of both was to be construed as a matter of EU law: Article 23 and s.13 had an autonomous meaning, and were to be construed on the basis that they were giving effect to the right to privacy under the **ECHR** art.8 and the right to protection of personal data in the **Charter** of Fundamental Rights of the European Union art.8
- In analogous decision in *Gulati v MGN Ltd* [2015] EWCA Civ 1291, damages were awarded for the **loss of the right to control formerly private information** which derived from the same core right to privacy
- **A person's control over data or over their browser generated information did have a value**, so that the loss of that control also had a value → damages were capable of being awarded for loss of control of data, **even if there was no pecuniary loss and no distress**

ICO's investigative powers (s 115, arts 57-58)

a. To order the controller and the processor and, where applicable, their representative to **provide any information** it requires for the performance of its tasks
b. To carry out investigations in the form of data protection **audit**;
c. To carry out a review of data protection **certifications** issued pursuant to art.42(7) of the UK GDPR;
d. To **notify** the controller or the processor of an alleged **infringement** of the UK GDPR
e. To obtain, from the controller and the processor, **access to all personal data** and to all information necessary for the performance of its tasks
f. To obtain access to any **premises** of the controller and the processor, including to any data processing equipment and means, in accordance with EU and Member State procedural law

ICO's corrective powers (art 58(2))

a. To issue **warnings** to a controller or processor that intended processing operations are likely to infringe the UK GDPR
b. To issue **reprimands** to a controller or a processor where processing infringes UK GDPR
c. To order a controller or a processor to comply with a data subject's **requests to exercise their rights**
d. To order the controller or processor to **bring processing operations into compliance** with the provisions of the UK GDPR
e. To order the controller to communicate a personal data **breach to the data subject**
f. To impose a temporary or definitive limitation including a **ban on processing**
g. To order the **rectification** or **erasure** of personal data or restriction of processing and the notification to recipients to whom the personal data have been disclosed
h. To withdraw a **certification** or to order the certification body to withdraw a certification or to order the certification body not to issue a certification if the requirements are not /no longer met
i. To order the **suspension** of data flows to a recipient in a **third country** / international organisation
j. To impose an **administrative fine**

Sanctions

- Administrative fines (Art. 83) - Two-tiered approach
- **For certain infringements including breaches of basic principles of processing, conditions for consent, breaches of data subject's rights and provisions regarding transfer to 3rd countries**:
  - Up to the greater of **4% of global turnover or 20 million Euros** (spot rate of exchange set by the Bank of England on the day on which the monetary penalty is imposed, s. 157)
- **For other infringements: up to the greater of 2% of global turnover or 10 million Euros**
- In January 2021, research by DLA Piper reported that an overall total of €272m has been levied in fines by European data protection authorities (in July, Lux £746m against Amazon)
- Alongside administrative fines, **corrective powers** of supervisory authorities (Art. 58) e.g. **to order the controller or processor to bring processing operations into compliance with the GDPR in a specified manner and within a specified period**

Deterrent?

- **A key function of GDPR sanctions is deterrence. It has been argued that truly dissuasive administrative fines must be issued in order for the sanctions to have their necessary deterrence effect;** this is in part due to the fact that - despite the overall rise in fines - the Irish Data Protection Authority (the Data Protection Commission or DPC) is the "*lead authority for most of the U.S. Tech Giants, and it has* ***failed to act against them up to now, resulting in a potential lack of deterrence***" (Voss and Bouthinon 2020)

Criminal offences

- Under s.170 of the DPA, it is a criminal offence for a person to knowingly or recklessly **obtain, disclose or procure the disclosure of personal data** without the consent of the controller or, after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained
- Under s.171(1) of the DPA, it is a criminal offence for a person knowingly or recklessly to **re-identify information that is de-identified** personal data without the consent of the controller responsible for de-identifying the personal data
- **Where a request has been made in exercise of a data subject access right and data portability right, and the person making the request would have been entitled to receive information in response to that request, it is a criminal offence under s.173 of the DPA to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of information that the person making the request would have been entitled to receive**

Privacy law remedies

- Interdicts/injunctions
- Compensatory damages
- Account of profits
- Delivery-up
- Proportion of costs

Compensatory damages

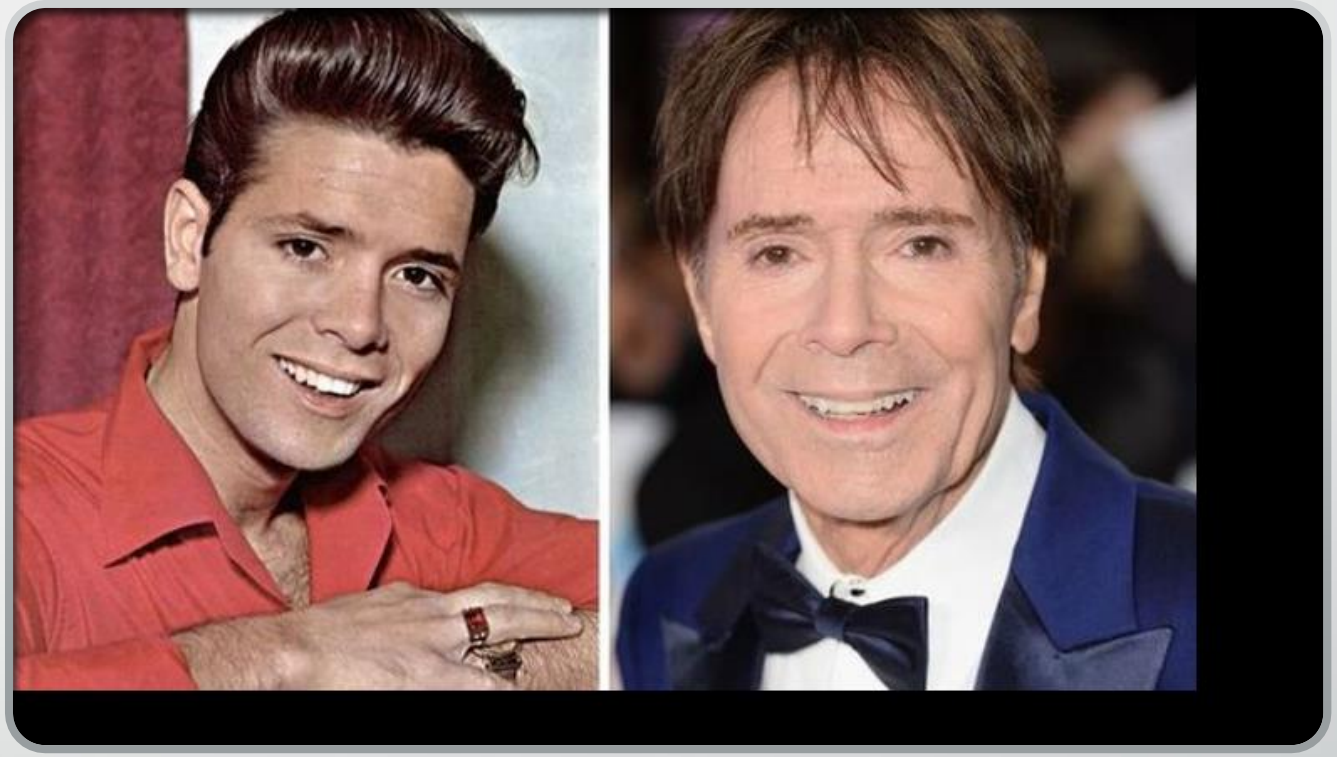
- Compensatory damages can include:
  - Special damages for **actual pecuniary loss** which is capable of being estimated in money
  - Aggravated damages (if aggravating circumstances exist), meaning additional damages to provide compensation for **mental distress** or injury to feelings caused by the manner or motive with which a wrong was committed or by the defendant's conduct subsequent to the wrong

Damages and reputation – *Richard v BBC*

- *Richard v BBC* [2018] EWHC 1837 (Ch), Sir Cliff Richard's high-profile case against the BBC for breach of privacy and data protection rights, arising out of the BBC's coverage of a police raid on his home in relation to a police investigation into an allegation of historical sex abuse
- Regarding the **balancing** of the competing Article 8 and 10 rights, applying the criteria set forth by the ECtHR in *Axel Springer*:
  - While the report of an investigation into a well-known but unidentified celebrity in relation to allegations of historical sexual abuse would contribute to a **debate of general interest**, this **did not require the identification of the individual involved**
  - The BBC had **obtained the information in a "questionable" way**
  - Significant degree of "breathless **sensationalism**" in the way the BBC presented the story
- Mann J concluded that Sir Cliff's privacy rights were **not outweighed by the BBC's rights to freedom of expression**, the most significant factors being:
  - The very serious **consequences of disclosure** for a person such as Sir Cliff, including the stigma attached to the revelation, magnified by the nature of the allegations against him
  - The **style** of reporting

Damages and reputation – *Richard v BBC*

- Regarding damages, Mann J held that the BBC should pay **general damages, including aggravated damages, of £210,000**.
- He held that, as a point of principle **damages should be available for an invasion of privacy resulting in damage to reputation**



Injunctions

- In *Bull v Desporte* [2019] EWHC 1650 (QB), the court granted a **permanent injunction** restraining the publication of a book about the author's sexual relationship with a National Lottery winner and awarded **damages** for misuse of private information and unauthorised use of photographs.
- The injunction was seen as the appropriate remedy for violation of the claimant's art.8 ECHR rights and to prevent the defendant from publishing the information much more widely, as was her intention.

One of UK's biggest EuroMillions winners brings restraining order against ex-mistress

Online injunctions

- *BVC v EWF (No. 2)* [2019] EWHC 2506 (QB) the parties were in a same-sex relationship, they broke up, D set up a website where he disclosed details of the relationship, the C's sex life, his health and finances, and allegations of wrongdoing.
- **Homosexuality is illegal** in the countries where the C was born and where he moved and therefore wanted to keep the information secret.
- **Information about sexuality**, sexual behaviour, health, finances and private and family life, was at the core of the ECHR art.8 protections.

- It made no difference whether some people already had the information: the question was not whether information was generally accessible, but **whether an injunction would serve a useful purpose** (see PJS v News Group Newspapers Ltd [2016] UKSC 26)
- Publication would not contribute to a debate of **general interest**: C was not a public figure and the information concerned private matters
- While there was a right to tell one's story, the D's story could be told without the website's intrusion into the C's private life (O v A [2015] UKSC 32). **Therefore, the claimant was entitled to damages and an injunction regarding internet publication of his private information** (his 'centre of main interests' was in England, see Bolagsupplysningen OU v Svensk Handel AB (C-194/16) [2018] Q.B. 963)

References

- *Durant v Financial Services Authority (Disclosure) [2003] EWCA Civ 1746; [2004] F.S.R. 28* - meaning of "personal data" (restrictive interpretation) and the meaning of "relevant filing system".
- *Johnson v Medical Defence Union Ltd [2004] EWHC 347 (Ch)* - meaning of "personal data" (applies Durant, above).
- *Chief Constable of Humberside v Information Commissioner [2009] EWCA Civ 1079; [2010] 1 W.L.R. 1136*
- *Vidal-Hall v Google Inc [2014] EWHC 13 (QB); [2014] 1 W.L.R. 4155*
- *Lloyd v Google LLC [2018] EWHC 2599 (QB)*
- *WM Morrison Supermarkets Plc v Various Claimants [2018] EWCA Civ 2339*
- *R (on the application of Bridges) v Chief Constable of South Wales Police [2019] EWHC 2341 (Admin)*
- *Naomi Campbell v Mirror Group Newspapers* [2004] UKHL 22
- *Douglas v Hello! Ltd (No.8)* [2007] UKHL 21
- *Browne v Associated Newspapers Ltd* [2007] EWHC 202 (QB)
- *Beckham & Another v News Group Newspapers Ltd* [2005] EWHC 2252 (QB)
- *John Terry v Persons Unknown* [2010] EWHC 119 (QB)

Mosley v UK, Application no. 48009/08; [2012] EMLR 1