11KBW

Data Protection etc: Some recent developments

Robin Hopkins

An agenda

11KBW

- Early(ish) days in the GDPR era. Some hugely important evolutions:
  - Civil litigation: AP QC
  - EU developments: JM QC
  - Brexit and tech frontiers: TPP QC

- This session focuses on other (mainly domestic) developments that shed light on some ‘every day’ DP issues, like:
  - Personal data
  - Controllership
  - Procedural safeguards
  - SARs
  - Data-sharing arrangements
  - Enforcement

Bridges: justifying privacy intrusions

11KBW

- *R (Bridges) v Chief Constable of South Wales Police and Others* [2019] EWHC 2341 (Admin)
  - Challenge to police use of automated facial recognition technology
  - Claim dismissed: privacy intrusion justified under Art 8(2) ECHR and no breach of DPA

- Key points from the ECHR claim:
  - There was a significant privacy intrusion – especially because biometric data involved
  - But this accorded with an adequate legal framework: law, guidance, etc.
  - And the intrusion was limited and proportionate

Bridges: personal data

11KBW

- Personal data when you don't know or care who someone is? (see paras 115-127 of the judgment)

- Either indirect identifiability
  - See e.g. *Breyer* principles: not personal data "if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant"

  - Or individuation/singling out:
    - See e.g. *Vidal-Hall* discussion of business models predicated on individuating users and treating them differently

A personal data interlude

11KBW

- While we're on the scope of personal data, remember the useful insights offered in *Lonsdale v Natwest* [2018] EWHC 1843 (QB):
  - Dispute included a SAR about bank's decisions to freeze an individual's accounts

- Personal data can include:
  - Info on bank's suspicions: what did it regard as suspicious activity and why?
  - Info on bank's decision-making about him/his accounts
  - Info on bank's meetings about him – including attendees

Bridges: sensitivity & proportionality

11KBW

- Biometric data is ‘sensitive’/’special category’ data

- No breach of DPP1:
  - Processing in accordance with an adequate legal regime
  - Transparency adequate: posters, Facebook, Twitter feeds, etc.
  - Purpose limitation
  - Limited reach
  - Limited processing activities
  - Limited prejudicial consequences in practice
  - Granular retention periods

- ‘Strict necessity’ test passed, based on proportionality analysis

Bridges: DP procedural safeguards

11KBW

- Appropriate policy documents:
  - Court reluctant to intervene
  - Law prescribed broad generic steps, and no detailed guidance to help

- DPIAs and the Court's scrutiny (para 146):
  - *"What is required is compliance itself, i.e. not simply an attempt to comply that falls within a range of reasonable conduct... However, when conscientious assessment has been brought to bear, any attempt by a court to second-guess that assessment will overstep the mark."*
  - A (non-Bridges) example in practice: see National ANPR service's published DPIA (https://www.gov.uk/government/publications/national-anpr-service-data-protection-impact-assessment)

Fashion ID: data controller(s)

11KBW

- *Fashion ID* CJEU judgment (Case C-40/17; July 2019):
  - Online retailer embeds Facebook 'like' button
  - Retailer can be a controller re transmission of personal data to Facebook

- Key consideration 1 – influence:
  - *"A natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller"*: see e.g. *Jehovan todistajat* (C-25/17) and *Facebook 'Fan Pages'* (C-210/16)

- Key consideration 2 – commercial (or other) benefit

Fashion ID: dividing responsibilities

11KBW

- *Fashion ID* is an 'old law' DP case, but sheds light on joint controllership per Art 26 GDPR:
  - *"joint liability does not necessarily imply equal responsibility"*
  - "*operators may be involved at different stages of that processing of personal data and to different degrees, with the result that the level of liability of each of them must be assessed with regard to all the relevant circumstances of the particular case"* (para 80)

- Online retailer only responsible for transmission of personal data to FB; not responsible for what FB did with that data

SARs & proportionality

11KBW

- *Dawson-Damer v Taylor Wessing* [2019] EWHC 1258 (Ch)
  - LPP issues, but more generally NB re search duties
  - Search of paper files ('relevant filing system') not disproportionate
  - Searching backup system would be disproportionate
  - Relevant points were that search results would contain personal data of others + confidential client information
  - But noted: appeal judgment awaited

- Fending off pre-action disclosure applications – SARs to the rescue?
  - *Hussain v MDU* [2020] EWHC 157 (QB): CPR 31.16 application
  - One factor in refusal: could get much of the material sought quickly via another route, i.e. a SAR

SARs: ICO draft guidance (1)

- Some points on timings:

- Comply within 1 calendar month (3 March > 3 April), even if received on a non-working day (though response date means next working day)

- Extension of up to 2 months if multiple requests or if ‘complex’:
  - Consider nature of organisation, technical difficulties, specialist input, exemptions, sensitivities/vulnerable data subjects
  - SAR is not complex solely because:
    - Large amount of info requested
    - You need to work with processors to comply

SARs: ICO draft guidance (2)

11KBW

- ‘Manifestly unfounded or excessive’?
  - Unfounded: no SAR intention; malicious intent, etc.
  - A SAR will not be excessive just because it encompasses a *“large amount of information, even if you might find the request burdensome (instead you should consider asking them for more information to help you locate what they want to receive)”*

- Bulk SARs are valid SARs:
  - *“If a request is made by a third party on behalf of an individual, the behaviour of the third party should not be taken into account in determining whether a request is manifestly unfounded or excessive”*
  - However: ICO will consider volume of requests, resources and procedures of the controller, etc.

Data-sharing arrangements: *M* (1)

11KBW

- *M v Chief Constable of Sussex* [2019] EWHC 975 (Admin):
  - JR re data-sharing between police and BCRP (business crime reduction partnership)
  - ISA (information-sharing agreements) both pre- & post-May 2018
  - Shared data included name, date of birth, photograph, bail conditions, apparent indicators re vulnerability & re criminal/anti-social behaviour

- ISA held to be lawful:
  - Appropriate technical & organisational measures in place to comply with DP principles (part 3 DPA 2018)
  - Factors: nature of data; nature of recipient; recipient's training and vetting duties; proportionality focus on children's rights & interests; data security measures; binding onward-sharing agreements

Data-sharing arrangements: *M* (2)

11KBW

- Sharing of M's data lawful in part:
  - Sharing of data (under DPA 98) re her vulnerability/risk of exploitation not justified
  - But other data-sharing justified (public protection, etc.)
  - Much of the data already known to BCRP

- Some other notable points:
  - A LIA was an NB part of the adequacy of the ISA
  - Police & BCRP were joint controllers, thus both responsible for any onward-sharing
  - Photograph = biometric data and thus special category

DP & privacy: some curiosities

11KBW

- *Mustard v Flower and Others* [2019] EWHC 2623 (QB):
  - Covert recording admissible: unethical, but relevant & probative
  - DP: ‘personal purposes’ + ‘legal proceedings’ exemption

- *BC & Others v Chief Constable of Scotland* [2019] CSOH 48:
  - No reasonable expectation of privacy in respect of group WhatsApp chats between police constables apparently implicated in misconduct investigation – based on their conduct and statutory regime relevant to police officers’ duties & expectations

ICO enforcement

11KBW

- Rise in number of ICO prosecutions for data offences

- Last stages of ‘old law’ MPNs:
  - *Facebook* appeal settled Oct 2019
  - Jan 2020 £500k DPA 98 MPN vs *DSG Retail* re malware cyber-attack

- *Doorstep Dispensaree* given £275k GDPR fine (December 2019):
  - Large volume of hard-copy prescription data stored insecurely in yard
  - Arts 5(1)(f), 24 & 32 (data security)
    - Attempt to blame data processor (document disposal service) dismissed
  - Art 5(1)(e) (retention periods)
  - Arts 13-14 (transparency notices)

- NOIs announced re *BA* and *Marriott*: further developments awaited