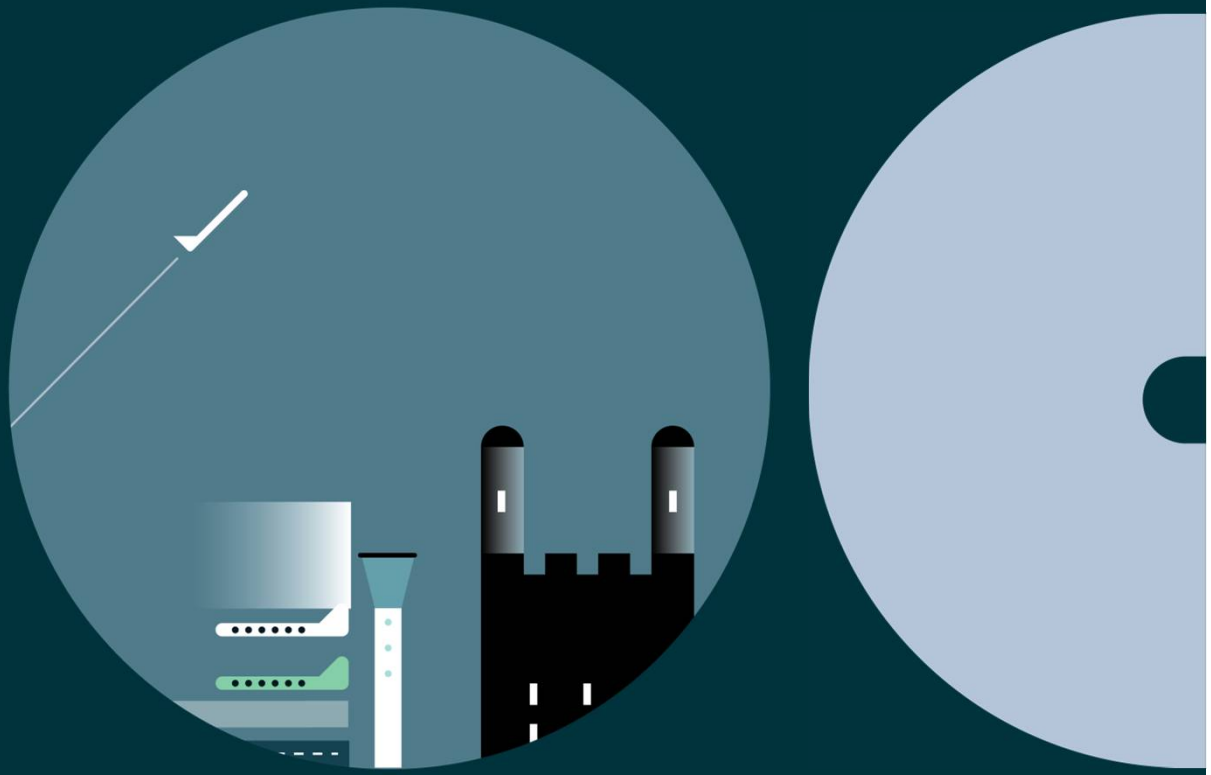
The EU is coming to get you

New risks for US businesses targeting Europe and exploding some EU data privacy myths

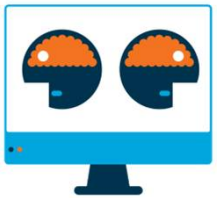
Stephen Groom



BAA Chicago

7 November 2014

What is this deck about?



- Exploding four myths around US marketers' current exposure to EU data privacy law
- Recent EU cases giving rise to new potential risks
- Attacks on "safe harbor" on three fronts
- More risks for US businesses around the corner

Exploding some myths #1

- *If our US head office is using a UK data processor to process personal data but this only relates to our US customers, EU data protection law cannot apply*
- **Wrong**
- Data Protection Directive 95/46/EC ("DPD") is engaged if
  - the data controller is not established in the EU, but uses equipment in the EU to process personal data other than for transit purposes…
  - so there is no requirement that the personal data relates only to EU residents

Exploding some myths #2

- *Our US website hosted on a US server runs online promotions which UK residents can enter*
- *So to avoid breaking EU laws on transferring personal data from the EU to the US we should sign up to safe harbor and include notice and consent provisions in the site privacy policy*
- **Wrong**
- Under the UK Data Protection Act 1998 ("DPA"), no "transfer" of personal data is occurring here such as to engage EU personal data export controls

Exploding some myths #3

- *Our UK subsidiary is running a sweepstakes on its website on a UK server targeting residents of France, Germany and the UK, then transferring the entrant data to us at head office in NYC where we will select the winner*
- *As we are all in the same group, the UK co doesn't need to worry about complying with DPD personal data transfer rules*
- **Wrong**
- Transfers of personal data between different legal persons, even if in the same group, will engage DPD data transfer rules

Exploding some myths # 4

- *In light of the answer in myth #3, to legitimise the transfer of personal data from the UK to the US, we should include consent wording in the UK site privacy policy and ensure the US co is certified under safe harbor*
- **Wrong**
- Safe harbor and consent are **alternative** ways of compliantly exporting personal data from UK/EU to the US
- Consent must be unambiguous, freely given, specific and informed, so consent unlikely to be achievable….
- so use either safe harbor or a data transfer agreement using EC-approved model terms

ECJ: C-131/12 Google/ Gonzalez, 13 May 2014 ("Google Spain")

The facts…

- in 1998 a Spanish newspaper published the na
  Spanish national as part of a story about the auction of a property to cover social security debts.
- When the individual's name was entered into Google Search in 2010, two links to the story appeared as search results.
- The individual lodged a complaint against Google, in which he requested the removal or redaction of his personal data from these links. Eventually, the case was referred to the ECJ.

Google Spain-what Google Inc said

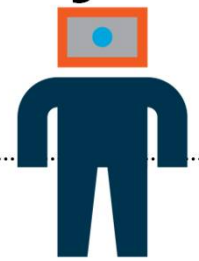
- Search engine activity is *not "processing"* of personal data because searches process all information on the internet without differentiation between what is and what is not "personal data"
- A search engine is *not a "data controller*" because it has no knowledge of the data processing and has no control over it
- Google Search is operated and managed by Google Inc in the US and claimants have *not established that Google Spain carries out in Spain any activity directly linked to the alleged data processing.*

ECJ: C-131/12 Google/ Gonzalez, 13 May 2014

Important findings (1)

- A search engine operator processes personal data within the meaning of Art. 2 lit. b of the DPD by
  - systematically searching the internet for (personal) information
  - organising the data within the framework of its indexing programmes,
  - storing it on its servers and
  - making it available to its users in the form of lists of search results
- search engine operators are data controllers, because they facilitate user's access to information, enabling them to establish a detailed profile on a data subject.

ECJ: C-131/12 Google/ Gonzalez, 13 May 2014



Important findings (2)

- Even if personal data is not processed within the EU, the DPD may still apply if the processing is deemed to have been processed "in the context of the activities" of an EU-based establishment of the controller
- It is sufficient in this respect, if the activities of the search engine operator and its EU subsidiary are "inextricably linked".
- The advertising and promotion activities of the subsidiary allow the search engine to operate and, vice versa, the existence of the search engine allows the advertising and promotion activities to be carried out.
- Therefore the processing of Gonzalez' personal data carried out by Google Inc was carried out "in the context" of the activities of Google Spain and…
- as data controller Google Inc was obliged to comply with the DPD

ECJ: C-131/12 Google/ Gonzalez, 13 May 2014 *key takeaways aside from RTBF*

- For the DPD to be engaged it is not necessary for processing of personal data to occur within the EU
- The processing just has to occur "in the context" of activities of a business of the controller established in the EU
- The ECJ judgment has opened the door to a much more liberal interpretation of "in the context"
- The key question is whether on the facts there is an "inextricable link" between the US and EU entities such that their relevant businesses are mutually supportive.
- Application to other service providers (e.g. social networks, data broker, online advertising networks)?

Vidal-Hall & others v Google Inc.

UK High Court Ref: [2014]EWHC 13 (QB)

The facts…

- Three English iPad users sued Google Inc in England for breach of the DPA and misuse of private information arising from Google's circumvention of Apple's "do not track" settings
- In the US numerous disputes arose from this circumvention and in 2012 Google paid a record USD 22.5m to the FTC and in 2013 USD 17m to AGs in 37 states
- The UK claimants argued that Google's tracking of their online activity without consent and use of it to serve online ads was a misuse of their personal data which also breached the DPA and caused damage
- In the form of distress and anxiety resulting from other people using the device seeing ads based on the claimants' online activity

Google's appeal against leave to serve English proceedings on them in US

How the court decided on Google's points

Google's submission

1. Claim not in tort so rules say there can be no service in US
2. Claim not for pecuniary damage sustained in England
3. Cookie-derived information from online activity is not "private information" or "personal data"
4. All documents and evidence relevant to Google's conduct and tracking were in California, so England not the most appropriate forum

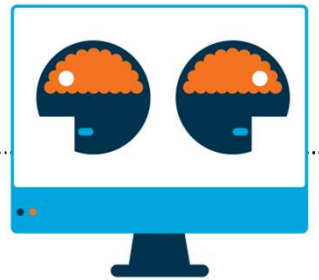
Tugendhat J's finding

1. "Misuse of private information" is a tort
2. Alleged damage is distress and anxiety occurring in England and suffices for these purposes
3. Google's submission "surprising"- claimant's position clearly arguable
4. Evidence largely electronic so use in England will not be problematic and real focus likely to be on damage suffered in England and complex English law issues, so England the best forum

The High Court's decision
Key takeaways

- The judgment may be appealed, but opens up new grounds on which US businesses may be exposed to privacy-based litigation by UK/EU residents
- even if the US entity has no nexus with an EU business and might think following Google Spain that it is therefore not exposed as there is no "processing in the context of the activities of an establishment of the controller" in the EU
- The judgment also opens up a new potential EU "do not track" battlefront for US businesses involved in OBA if behavioural data is regarded as "personal data" and the "distress and anxiety caused by third parties viewing behavioural ads" line of attack is sustainable.

Safe harbor under fire on three fronts



1. November 2013

In response to the "Snowden/NSA" revelations, the European Commission published 13 recommendations for improving safe harbor

2. June 2014

Irish High Court case [2014] IEHC 310 Maximilian Schrems vs Irish Data Protection Commissioner [and Facebook] Hogan J refers to the ECJ the question of whether the safe harbor regime introduced in 2000 should be re-evaluated in light of the 2009 EU Charter of Fundamental Rights (Article 8 on Protection of personal data)

3. August 2014

Center for Digital Democracy files complaint with the FTC and calls for 30 safe harbor-certified companies to be investigated

Draft Data Protection Regulation

- **Article 3**
- The Regulation applies to the processing of personal data by a controller or processor not established in the EU where the activities relate to:
- (i) the offering of goods or services to data subjects in the EU; or
- (ii) the monitoring of their behaviour
- NB "Nothing is agreed until everything is agreed"
- Current plan: finalise in 2015 and bring into force 2017

Further questions

Stephen Groom

Co-chair-Advertising & Marketing Law Group

Deputy Chair-Privacy and Data Law Group

T +44 (0) 207 105 7078

M +44 (0) 207 105 7079

stephen.groom@osborneclarke.com

www.marketinglaw.co.uk