11KBW

EU Developments: enforcement, legislation and guidance (including e-privacy)

Julian Milford

- National DP authorities across the EU grappling with many similar issues in interconnected world.

- So much happening, and so many important EU developments, that this talk cannot be comprehensive.

- Will deal with:
  1. Action by national authorities across the EU for GDPR breaches: consistency, the one-stop shop.
  2. The right to be forgotten or to have offending content removed and territorial reach of EU privacy legislation: *Google 2, GC, Glawischnig-Pisczek*
  3. E-Privacy: ePrivacy Regulation, *Planet49, Privacy International*
  4. *Schrems II:* A-G's Opinion
  5. Video surveillance and facial recognition: *M5A* and EDPB guidance

GDPR BREACHES: THE EU PERSPECTIVE

11KBW

- Major GDPR fines (100,000 euros plus) of around 430m euros issued in 2019 (including ICO's notices of intent vs BA and Marriott).

- The recent big GDPR/eprivacy fines?
  - £183m vs British Airways, ICO (July 2019 notice of intent – but no final outcome until 31 March 2020)
  - £99m vs Marriott, ICO (July 2019 notice of intent, but again, no final outcome until 31 March 2020)
  - 50 m euros vs Google, CNIL, January 2019 (but under challenge through French courts)
  - 28m euros by Italian DP authority vs TIM for unsolicited marketing calls, Feb 2020
  - 18 m euros by Austrian authority vs Austrian Post for selling 3m data
  - 14.5m euros by German DP authority vs Deutsche Wohnen for unlawful storage of old personal data, December 2019

A mixed picture…

- The most eye-catching fines not yet confirmed (and nothing standing comparison to 5bn Facebook fine in US)
- Lack of consistency across EU member states re size of fines and readiness to enforce.
- Consistency on the agenda: EDPB has power to set consistency guidelines (Art 70(1)(k) GDPR) though has not yet done so.
- Two nations most directly responsible for policing the tech sector – Ireland and Luxembourg – have not yet completed any sizeable investigation of US tech firm.

Of course, size of fine may not be major issue…

11KBW

- Finding of breach in relation to significant cohort opens door to civil litigation (e.g. British Airways)

The particular problems of policing tech

11KBW

- Principle of one-stop shop under Art 56 GDPR requires supervisory authority of the main establishment/single establishment of the controller/processor within the EU to act as lead supervisory authority for cross-border processing

- Irish regulator oversees Google, Facebook, Microsoft, Twitter, LinkedIn, Apple, Airbnb, Dropbox (among others) with limited budget (16.9m euros in 2020) .

- Irish regulator carrying out number of large investigations including into WhatsApp, Facebook, Google. But no decisions at all yet issued.

- Similar issues e.g. in Luxembourg re investigation of Amazon

- Cooperation procedure in Art 60 GDPR yet to be tested.

Decisions to look out for?

11KBW

- From Irish DPA, there are around 20 open statutory inquiries into US tech companies registered in Ireland, including:
- Statutory inquiry into Google's processing of location data, and transparency surrounding that processing (launched Feb 2020)
- Statutory inquiry into Google concerning personalised online advertising (still outstanding from May 2019)
- Statutory inquiry into Twitter re data breach notification (investigation finished in October 2019, but draft decision not yet issued)
- Statutory inquiry into WhatsApp re sharing of personal data with parent company Facebook (investigation finished in October 2019, but draft decision not yet issued)

Can a regulator bypass one-stop shop…?

11KBW

- In January 2019, CNIL levied fine of 50m on Google re ads personalisation and lack of transparency/valid consent
- Google's EU HQ in Dublin; but CNIL found Irish establishment had no decision-making power on processing operations in Android system concerning ads personalisation. Because decision-maker was Google LLC, CNIL considered itself competent to take any decision regarding its processing, as were other DPA
- Google has appealed. No outcome yet.
- However, CNIL fine hasn't been general prompt for other bypassing of one-stop shop. Other national regulators (e.g. Swedish and Dutch authorities) have passed complaints about Google/Microsoft to Irish DPA.
- Not yet any joint operation between different EU regulators under Art 62 GDPR

Another possibility: acting in a case of "urgency"

11KBW

- Art 66(1) GDPR contains an "urgency procedure" allowing derogation from one-stop shop mechanism where there is an *"urgent need to act in order to protect the rights and freedoms of data subjects"*

- Limited to *"provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months"*

- The Hamburg DP Commissioner used this process when opening administrative proceedings against Google on 1 August 2019 re speech assistance systems (employees of Google listened to voice recordings to analyse the effectiveness of its Home Speech Assistant). Procedure halted on 26 August after Google agreed changes to processes.

- See also Art 66(3) GDPR, and request urgent opinion or binding decision from EDPB

And who is the lead authority if controller moves?

11KBW

- EDPB Opinion 8/2019
- Essentially, the relocation of the main establishment to the territory of another EEA member state mid-procedure deprives the first authority of original competence, albeit not retrospectively, from the moment that the move is effective. That applies right up until a final regulatory decision.
- The rationale is the need for effective enforcement, and clarity of application
- The Opinion says that its test is designed to prevent forum shopping, but query whether that is so

Post Brexit...

- ICO will no longer be part of EU enforcement mechanism. So one-stop shop issues will not arise in UK: UK will be responsible for breaches within its jurisdiction.

DEREFERENCING AND RIGHT TO BE FORGOTTEN

11KBW

- 3 important CJEU cases in late 2019 concerning the rights of data subjects to request dereferencing of search results, or removal of offending content on social medial platforms, relevant to the powers/duties of national DP authorities:
  - (1) *Google LLC v CNIL C-507/17* [2020] EMLR 1 (24 September 2019, Grand Chamber)
  - (2) *GC v CNIL C-136/17* (24 September 2019, Grand Chamber)
  - (3) *Glawischnig-Pisczek v Facebook Ireland Limited C-18/18* (3 October 2019)

Google v CNIL

- Concerns a decision of CNIL on dereferencing requests made in 2015 i.e. Directive 95/46, but CJEU also addressed position under GDPR Art 17 (i.e. the right to be forgotten)

- Are search engine operators required, when granting a request for dereferencing, to apply it to all of the domain names used by the search engine, so that links no longer appear, irrespective of the place from where the search is conducted, even if that place is outside the EEA?

- If not, does dereferencing only apply to the domain name corresponding to the state in which the request is made?

- And if dereferencing applies e.g. only in the EEA, must the search engine operator use ”geo-blocking” of all search results, where the search is in EEA?

Google v CNIL (2)

- I.e. if you ask for dereferencing in UK, must Google remove (i) .co.uk results only; (ii) results in EU; or (iii) results worldwide?

- And if you ask for dereferencing in UK, must Google ensure any search carried out in the UK would not be able to get results from any domain name worldwide (or at least, any domain name in the EU)?

- CNIL contended that for the right to be effective, Google must delist universally.

Google v CNIL (3)

- Court held that search engine operators do not have any obligation in EU law to carry out a dereferencing request on all the versions of their search engines: [64]. Request applies to all Member States, in order to maintain a high level of protection throughout the EU: [66]. But not worldwide.

- Judgment reflects the balance of competing interests. CJEU recognized that in a globalized world, interests of EU data subjects are affected by searches taking place anywhere, and in respect of any domain name: which tends towards need for global dereferencing.

- But equally, CJEU recognized that numerous third States do not recognize any right to deferencing or have a different approach to that right: [59].

Google v CNIL (4)

11KBW

- Judgment implicitly recognizes the danger pointed out by Advocate-General that if worldwide dereferencing were required, there could be real dangers for freedom of information:

"There is a danger that the Union will prevent people in third countries from accessing information. If an authority within the Union could order a global deference, a fatal signal would be sent to third countries, which could also order a dereferencing under their own laws…There is a real risk of reducing freedom of expression to the lowest common denominator across Europe and the world."

Google v CNIL (5)

11KBW

- CJEU pointed out that the balance of competing rights and interests in accessing information might vary from one Member State to another, and weighing up of interests would not necessarily be the same. So national supervisory authorities would need to cooperate under Arts 56 and 60 GDPR to reach a binding consensus which would cover all searches in territory of the Union: [69].

- The search engine operator would also need to take measures which had *"the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name"*: [70].

Google v CNIL (6)

11KBW

- “Seriously discouraging” is not expanded upon: no explanation of what this might mean in technical terms (whether geoblocking or something else)

- But in practice, search engines have worked since 2014 to block access to delisted URLs via other country search domains, when accessed from the country that requested delisting. Judgment affirms that process within EU.

Google v CNIL (7)

11KBW

- Sting in the tail: the judgment explicitly does not preclude national authorities from applying their own more stringent standards, and requiring universal delisting. See [72]:

- *"…it should be emphasized that, while…EU law does not currently require that the de-referencing request granted concern all versions of the search engine in question, it also does not prohibit such a practice."*

Google v CNIL (8)

11KBW

- Tension between [72] of the judgment, and the judgment's own emphasis on cooperation between national authorities under Art 60.

- And difficulty in reconciling this approach with aim of GDPR to set common standards

- Also, raises the spectre of forum shopping in delisting requests. And arguably applies "floor not ceiling" approach to EU rights in an area where it is inapposite i.e. one that calls for balancing of competing rights that needs to be assessed on EU level.

GC v Google

11KBW

- Second important judgment of Grand Chamber on same day

- CNIL refused to serve 4 dereferencing requests on Google.

- Request from GC was for delisting of photomontage referring to a sexual relationship between her and a mayor of municipality whom she served as head of cabinet
- Request from AF for delisting of link mentioning him as PR officer in Church of Scientology
- BH asked for dereferencing of links re investigation linking him with funding of political party
- ED wanted dereferencing of links regarding criminal conviction for sexual assault

- The issue: how does dereferencing request apply to sensitive category personal data under Art 9 GDPR and criminal conviction data under Art 10?

GC (2)

11KBW

- First question: does search engine operator need to have a basis for processing special category personal data or criminal convictions data within Arts 9 and 10 GDPR?

- Answer: yes. As the CJEU pointed out at [44], any other conclusion would run counter to the purpose of Arts 9 and 10 to provide particular protection for data, the processing of which may involve serious interference with data subjects' fundamental rights under Arts 7 and 8 of the EU Charter.

- But judgment emphasizes that search engine operators aren't in same position as website operators who host content. They don't have to proactively police the net: they only need to consider restrictions when a data subject requests it: [47].

GC v Google (3)

11KBW

- The answer to Question (1) may have been unsurprising, but it's not immediately easy to see what Art 9 condition is met by a search engine operator.

- The judgment assumes it will generally be Art 9(2)(g) ("*processing is necessary for reasons of substantial public interest*"): see [61], [66]. But the "substantial public interest" is not Google's own. It is the right of freedom of information of internet users: [66].

- As the judgment implies at [63], the only other realistic possibility as regards a search engine operator would be Art 9(2)(e) (data manifestly made public by the data subject).

GC v Google (4)

11KBW

- It is at least logically awkward to treat Google's processing as being "necessary" for interests that are not Google's own. But the GDPR requires that analysis.

- The analysis allows for a balancing exercise between freedom of information rights, and the rights of data subjects under Arts 7 and 8 of the EU Charter: an exercise parallel to that in *Google Spain.*

- The judgment says that the balancing exercise will need to take into account the particularly serious interference with the data subject's rights, because of the sensitivity of the data: [67]. That means inclusion of the link must be "*strictly necessary*" for protecting the freedom of information of internet users: [68]. But judgment is otherwise non-prescriptive.

Glawischnig-Piesczek v Facebook

11KBW

- G-P case considers some similar issues to *Google v CNIL*, but in context of Directive 2000/31 (E-Commerce Directive).

- G-P complained to about an article on a Facebook user's personal page which defamed her, and was publicly accessible.

- The Austrian regional court required Facebook to remove the original content; and to remove equivalent content (but only where brought to Facebook's attention).

Glawischnig (2)

11KBW

- The questions referred by Austrian Supreme Court concerned Art 15 of the Directive (*"Member States shall not impose a general obligation on providers…to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity"*).

- Long-used by social media providers to say that they only need to remove specific illegal content identified by complainant or court.

- Question: could Facebook be ordered to remove not just the offending post, but (i) other identically worded information; and (ii) other information of equivalent content? And if so, was the obligation proactive? And did it extend to the Member State; or was it worldwide?

Glawischnig (3)

11KBW

- *First,* CJEU said that a host could be required to remove all identical information, irrespective who posted it, and without it being brought to the host's attention. That did not amount to "general monitoring". See [37].

- *Secondly,* a host could also be required to remove information of equivalent content, and to do so proactively: but only if the specific elements of the information are clearly stated in the injunction: [45]-[46]

- Host can't be required to carry out an *"independent assessment of content"*

Glawischnig (4)

11KBW

- The Court said that Directive 2000/31 didn't preclude worldwide injunctions, but didn't require them. It was up to Member States to ensure that their measures were consistent with public and private international law.

- Directive 2000/31 itself doesn't contain any geographic limitation.

E-PRIVACY

11KBW

What has happened to the ePrivacy Regulation?

- Intended to replace ePrivacy Directive at same time as GDPR replaced Directive 95/46/EC.
- Member States still cannot agree on content. Latest draft proposed by Finnish presidency failed to gain sufficient support on Committee of Permanent Representatives on 22 November 2019.
- Divergence on number of issues, including whether the investigation of serious crimes generally should warrant exemption from Regulation.
- Unlikely therefore that the ePrivacy Regulation will come into force before 2023 (at least).
- So for foreseeable future, PECR will continue to govern ePrivacy breaches.

E-Privacy and Consent: *Planet49*

11KBW

- Under Art 7 GDPR, consent as a basis for processing means clear, explicit, active, informed consent which must be demonstrated by the data controller. Pre-ticked boxes, silence or inactivity are no good.

- CJEU has confirmed that the same concept of consent applies within the ePrivacy Directive: see *Planet49 GmbH C-673/17.*

- This maintains alignment between ePrivacy Directive and DP law (see Art 2(f) of ePrivacy Directive – *"consent by a user or subscriber corresponds to the data subject's consent in Directive 95/46"*)

Planet49 cont.

11KBW

- Art 5(3) of ePrivacy Directive requires consent to cookies:

  "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information…"

- Result of application of GDPR definition of consent? Preselected tickbox used by website lottery didn't amount to valid consent under Art 5(3) of ePrivacy Directive for use of cookies.

Planet49 cont.

11KBW

- Important point from Planet49 that active consent of end user is required under Arts 2(f) and 5(3) of ePrivacy Directive, irrespective whether the information stored or accessed is personal data. See judgment, [71].

- This diverges from Commission's proposal for ePrivacy Regulation, which was that cookies used only to process information anonymously should no longer require end-user consent. So this aspect of ePrivacy Regulation unlikely to be taken forward.

Privacy International – A-G's Opinion

11KBW

- A-G's Opinion delivered in very significant case under ePrivacy Directive – *Privacy International v SSFCO, SSHD and GCHQ C-623/17*

- Case results from IPT reference following PI's challenge to acquisition and use of bulk CD by Security and Intelligence Agencies under DRIPA
- IPT referred questions:

1. Whether requirement that CSP provides bulk CD to a SIA falls within scope of EU law at all;
2. If so, whether any of the requirements in *Watson/Tele2* apply to the provision of bulk CD to a SIA (and if not, what requirements apply)

Privacy International – A-G's Opinion

11KBW

- A-G's Opinion delivered in very significant case under ePrivacy Directive – *Privacy International v SSFCO, SSHD and GCHQ C-623/17*

- Case results from IPT reference following PI's challenge to acquisition and use of bulk CD by Security and Intelligence Agencies under DRIPA
- IPT referred questions:

1. Whether requirement that CSP provides bulk CD to a SIA falls within scope of EU law at all;
2. If so, whether any of the requirements in *Watson/Tele2* apply to the provision of bulk CD to a SIA (and if not, what requirements apply)

Privacy International (2)

11KBW

- The *Watson* requirements?

- *Watson* ([2017] QB 771) concerned the Data Retention Directive. One of CJEU's most impenetrable and frankly impractical judgments. Exactly what it decided is unclear, but it held that DRD was contrary to EU law, and that as a minimum:
- (1) data retention cannot be "general and indiscriminate";
- (2) In a crime context, only the objective of fighting "serious crime" could justify retention;
- (3) Access to data would need to be granted only to the data of individuals suspected of being involved in serious crime;
- (4) Access must be subject to prior review by a court or other independent body.

Privacy International (3)

11KBW

- IPT referred the case with very strong steer as to what it thought the answer should be. It said the receipt of BCD, and its interrogation for "unknown unknowns", was *"essential to the work of the SIAs in countering serious threats to public security, particularly terrorism, espionage and nuclear proliferation. The SIAs' capabilities to acquire and use the data are essential to the protection of the national security of the United Kingdom".*

- *"The national court has found that the imposition of the requirements specified in Watson, if applicable, would frustrate the measures taken to safeguard national security by the SIAs, and thereby put the national security of the United Kingdom at risk."*

Privacy International (4)

11KBW

- A-G has essentially ignored the strongly-expressed concerns of IPT

- A-G's position?
- (1) Even if work of SIAs themselves is outside scope of EU law, requirement imposed on CSPs to retain data for SIAs is covered by EU law.
- (2) The *Watson* requirements can and should be read across to this sphere. I.e. national legislation should allow access only "*to the data of persons suspected of planning, of being about to commit, of having committed, or of being involved in, acts of terrorism*".
- (3) Access to data must be subject to prior review by a court/independent body.
- (4) Affected parties must be notified of access, unless that would compromise measure.
- (5) Data must be retained within EU.

SCHREMS II

11KBW

- Opinion of A-G delivered on 19 December 2019 in Schrems II (*Data Protection Commissioner v Facebook Ireland Limited C-311/18*)

- Very important case on validity of standard contractual clauses for data transfer to US. Facebook chose to rely on SCCs to legitimitize its EU-US data flows, following invalidation of Safe Harbor Framework in Schrems I.

- Mr Schrems not only challenges SCCs, but also requests that EU-US Privacy Shield be declared invalid.

Schrems II cont.

11KBW

- A-G Saugmandsgaard's Opinion is based on the nature of SCCs.

- Fact that they place responsibility on exporter and/or Member State supervisory authorities, and are not binding on the authorities of the third country of destination, does not render SCCs invalid. The issue is whether there are sufficiently sound mechanisms to ensure that transfers are suspended or prohibited where SCCs are breached: [124]-[128].

- I.e. SCCs need to be distinguished from adequacy decisions. The point of an adequacy decision is to find that a third country ensures equivalent protection to the EU. The obligations in SCCs are designed to operate precisely where the safeguards in the third country are NOT adequate/equivalent: [120]

A-G goes on to find that SCCs provide sufficient enforceable remedies against exporter and rights to remedy before Member State supervisory authorities: [130]-[150].

Schrems II cont.

11KBW

- Underlying all the A-G's conclusions is the point that *"the validity of [Decision 2010/87 on SCCs] does not depend on the level of protection that exists in each third country to which data might be transferred on the basis of the SCCs which it sets out"*: [158]

- The headline, therefore is "SCCs are valid".

- But there is a massive sting in the tail. The Opinion makes it clear that it would be for exporters/Member States to prevent/suspend transfers under SCCs to a country which did not provide an equivalent level of protection for DP rights in any specific case: [126].

- AND it sets out A-G's view that US does not provide equivalent protection

Schrems II cont.

11KBW

- A-G's views on US privacy protections are set out in lengthy and expressly *obiter* section on Privacy Shield, where he makes *"some non-exhaustive observations on that subject"*: [187] et seq

- A-G focuses on requirements of s.702 FISA and Executive Order 12333 in US (those being the main legal authorities relied on to collect intelligence information about foreign nationals).

- Among other matters, A-G says he doubts whether EO 12333 is "*sufficiently foreseeable to have the quality of "law""* AT ALL: [266]. And he says that it may be doubted whether s.702 FISA lays down sufficiently precise criteria for collection of data: [297] et seq.

- Also, A-G doubts whether Ombudsperson mechanism in Privacy Shield provides an effective remedy before an independent body.

VIDEO SURVEILLANCE / FACIAL RECOGNITION

11KBW

- National authorities and CJEU have been grappling with issues of video surveillance (including facial recognition)

- Early draft of EU White Paper on Artificial Intelligence, published on 19 February, suggested that Commission was seeking temporary ban on facial recognition in public places. The ban is not included in the published White Paper, which is relatively vague on privacy issues.

- This is another area rife with possible inconsistency between national authorities. See e.g. the contrast between Swedish DPA (which fined municipality around 20k euros for using facial recognition technology to monitor school attendance) with more liberal attitude of High Court in *R(Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341.

Video Surveillance: *TK v M5A C-708/18*

11KBW

- CJEU takes relatively pragmatic attitude to video surveillance in *M5A*, where owners' association installed video cameras in common parts of block of flats.

- TK challenged installation as breach of Arts 7 and 8 of EU Charter and Art 7(f) of Directive 95/46 (i.e. "legitimate interests" basis for data processing)

- CJEU says that national provisions may properly authorise surveillance of this type, the lawfulness of which depends upon the balance of interests in the particular case.

EDPB guidance on video monitoring

11KBW

- EDPB has recently issued "*Guidelines 3/2019 on processing of personal data through video devices*" (adopted 29 January 2020)
- Contains helpful guidance on when monitoring is and is not likely to be proportionate, as well as transparency/storage/erasure
- Problematic areas include range of devices for monitoring public spaces e.g. dash cams (esp if constantly monitoring traffic) as well as video surveillance by businesses and individuals
- Facial recognition techniques involving biometric recognition covered by the Guidance (which says they will in most cases require explicit consent under Art 9(2)(a) GDPR)