Twitter Thread by Robin Berjon

Robin Berjon
@robinberjon

Recently, the @CNIL issued a decision regarding the GDPR compliance of an unknown French adtech company named "Vectaury". It may seem like small fry, but the decision has potential wide-ranging impacts for Google, the IAB framework, and today's adtech. It's thread time! ■

It's all in French, but if you're up for it you can read:
• Their blog post (lacks the most interesting details): https://t.co/PHkDcOT1hy
• Their high-level legal decision: https://t.co/hwpiEvjodt
• The full notification: https://t.co/QQB7rfynha

I've read it so you needn't!

Vectaury was collecting geolocation data in order to create profiles (eg. people who often go to this or that type of shop) so as to power ad targeting. They operate through embedded SDKs and ad bidding, making them invisible to users.

The @CNIL notes that profiling based off of geolocation presents particular risks since it reveals people's movements and habits. As risky, the processing requires consent — this will be the heart of their assessment.

Interesting point: they justify the decision in part because of how many people COULD be targeted in this way (rather than how many have — though they note that too). Because it's on a phone, and many have phones, it is considered large-scale processing no matter what.

Other factor: the technicity and opacity of ad bidding systems is used to justify greater transparency requirements. People cannot expect to consent to what they don't understand (or even know exist), therefore the adtech ecosystem is de facto under *stronger* requirements.

The decision also notes that the @CNIL is openly using this to inform not just the company in question but whole ecosystem, including adtech of course but also app makers who embed ads and marketers who use them. You're all on notice!

Note that there is no fine: if Vectaury remediates by 1) no longer processing geographic data without consent, 2) retroactively wiping the data they have (since consent was invalid), and 3) prove they've done that then they're good to go.

Out of business, too, I would guess.

Fun fact: the @CNIL takes privacy seriously, and two years from now the Vectaury decision they have just made will be anonymised so that just the pure legal content remains.

Let's jump into the heart of it. The decision looked at two distinct but related aspects:

1) Consent obtained directly in apps that embed Vectaury as an SDK, using Vectaury's CMP (Consent Management Platform). You can see it in action in this video: https://t.co/LGOjNOD18d

2) Consent collected elsewhere and signalled to Vectaury through use of the @IABEurope Consent Framework.

Both are found to be failing — the second one in very interesting ways. Keep reading!

The CMP fails exactly as you would expect:

1) The consent is not informed;
2) The consent is not specific;
3) The consent is not affirmative.

Given the high-risk nature of the processing and its opacity, this isn't even a very strict interpretation.

Here is the bombshell though: Consent through the @IABEurope framework is inherently invalid. Not because of a technical detail. Not because of an implementation aspect that could be fixed. No.
You cannot pass consent to another controller through a contractual relationship. BOOM

Precisely: a controller has the obligation to demonstrate, for the entirety of the data they are processing under consent, the validity of the consent obtained. Otherwise you're just failing Article 7.

This is huge.

This means that if someone gains consent for you, and you have a contract saying it's their responsibility to do so, you *still* have the obligation to verify that the consent is valid.

This rules the @IABEurope out as an option, but more than that: @Google forced publishers to collect consent on its behalf for advertising profiling. They have said that they will audit that publishers do it right — but will auditing be enough?

The decision very specifically states the need to verify consent for the "entirety" of the data. By definition an auditing approach only does spot checking.

Also, Google has said they won't use a clear definition of valid consent. This shows they will have to.

So, yeah — that happened. It will be interesting to see how this lines up with @johnnyryan and @RaviNa1k's complaint about programmatic in terms of enforcement decision.

The one part that slightly disappoints me is that the decision does not call into question the role of Android and iOS in providing the ad ID and geolocation in the first place, as joint controllers, without proper consent.

That might be a fight for another day ■■