LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice

26 March 2019 | Number 2476

What Companies Can Learn From CNIL's Privacy Consent Cases on Targeted Marketing

The closure of four cases involving targeted advertising provides lessons for navigating compliance standards under the GDPR.

The recent closure of cases brought by the French Data Protection Authority (CNIL) against four French advertising technology companies for their privacy consent practices highlight opportunities for businesses at all layers of the adtech value chain to address emerging compliance challenges.

Whilst the requirements imposed by the CNIL may have appeared at first sight unduly burdensome to the adtech industry, they are unsurprising since they strictly align with the CNIL's interpretation of privacy obligations under the General Data Protection Regulation (EU) 2016/679 (GDPR).

Background

In 2018, the CNIL issued a warning against four French advertising technology companies — Fidzup, Teemo, Singlespot, and Vectaury. All four companies collect geolocation data from app users through a technology installed via third-party mobile applications downloaded by users. Once collected, the data is used to display targeted advertising. Vectaury also uses a real-time bidding system to buy advertising inventory within mobile applications that display campaigns.

After the CNIL decided to take action against these companies and issued its warnings, the nonprofit organization Privacy International filed a complaint against other adtech companies. The authority brought the complaint to three different European data protection authorities: the CNIL, the UK Information Commissioner, and the Irish Data Protection Commissioner. These complaints are currently under investigation.

The CNIL's Findings

The CNIL concluded in its warnings against Fidzup, Teemo, Singlespot, and Vectaury that the consent obtained from app users was invalid because:

- Consent was not informed: In each case, app users were asked to consent only to the collection of data by the provider of the mobile application itself, and not by the company providing the technology installed on the app for targeted advertising purposes. The CNIL also noted that the app began collecting geolocation data for targeted advertising purposes as soon as it had been downloaded, before users had been able to provide consent.

- Consent was not freely given: In each case, app users did not receive a clear option to refuse the collection of their geolocation data. For example, in the Singlespot case, the two alternatives available to the app users were either to "accept" or "to accept later." In the Fidzup and Teemo cases, the users did not receive the option to download the app without the tracking tool collecting the geolocation data being installed.

- Consent was not specific enough: App users could not consent *specifically* to the collection and use of their geolocation data for targeted advertising, as they only received the option to provide a single, general consent in relation to all data processing purposes. The CNIL considered this practice to be a breach of the principle that valid consent requires data subjects to be able to choose which purpose(s) they consent to, rather than being forced to consent to all purposes simultaneously.

Finally, in the case of Vectaury, the company had developed a consent tool with the support of an industry trade association — the International Advertising Bureau (IAB) — in order to collect consent for advertising purposes. The CNIL found that this consent tool used by Vectaury did not allow for specific consent for different purposes or provide sufficient information to users. In particular, the CNIL found that the information text displayed to the user lacked sufficient transparency, and was too complex, unclear, and imprecise. According to the CNIL, users were also not sufficiently informed of the identity of the companies that would receive their data, as this information was only available after several clicks.

In response to the CNIL's notice relating to Vectaury and the consent tool, as well as the suggestion by some commentators that the notice calls into question the IAB Europe Transparency & Consent Framework (TCF Framework),[1] the IAB publicly clarified[2] that Vectaury had also violated the TCF Framework in relation to many of the points on which the CNIL considered Vectaury to have violated the GDPR's consent-related requirements. The IAB insisted that, had Vectaury complied with the TCF Framework, not only would the company have met its obligations under the law, but it would have addressed most of the concerns raised by the CNIL.

As a result, the CNIL's warnings instructed the four companies to do both of the following within three months:

- Stop processing personal data for targeted advertisement purposes without a valid legal basis

- Delete all personal data obtained without valid consent

Closing of the Cases

By the end of 2018, the CNIL had closed the matters against Fidzup, Teemo, and Singlespot, as they had effectively changed their practices in compliance with the CNIL's requirements. On 26 February 2019, the CNIL publicly announced closure of the fourth and last case against Vectaury.

The CNIL's decision to close the cases was based on its findings that:

- The banner templates developed by the companies, to be displayed during the installation of the apps and before the collection of personal data, now allow the collection of an informed, freely given, and specific consent from app users.

- Specifically, these banners inform users of the purpose of the data collection (*i.e.*, targeted advertising based on geolocation), the identity of the data controllers receiving the data (accessible

via hyperlink), the data collected, and the option to withdraw consent at any time. The users can also access, via another hyperlink, additional information about their rights as data subjects.

- Regarding the real-time bidding system used by Vectaury, Vectaury now only processes personal data received from third parties' applications if the users' consent has been obtained, with Vectaury having committed to the CNIL to check in advance the conformity of the consent tool that is integrated in the partners' apps.

When deciding to close the case against Vectaury, the CNIL also noted that the new banner proposed by the company now includes:

- At a first level of information, a presentation of each processing purpose along with a button allowing the user to express consent for each purpose distinctly
- The presence of three different buttons allowing the user either to:
  - Accept all the purposes
  - Refuse them all
  - Save the choices made for each purpose

However, the stage at which the user can simultaneously accept or refuse all purposes remains unclear. For example, in Vectaury's case, this option appears to only be available when the user wishes to change his or her preferences, after having expressed consent for each processing purpose separately.

If the CNIL confirms that the user is unable to opt to "accept all" or "reject all" purposes when installing the app, both of the following could be negatively impacted:

- The interest of the users, who paradoxically could, by being offered too many choices, lose the right level of control over their data (as if they were not responsible enough to mindfully take the decision to "accept all" or "refuse all," at the same time)
- The rate of consents received by adtech companies, and therefore the business of such companies

Finally, the CNIL clarified that if the violations were to continue in the future, enforcement actions could be taken against these companies. These actions could ultimately lead to sanctions, including fines.

Key Takeaways

These cases provide helpful guidance to other adtech companies that are developing privacy compliance strategies. In particular, such companies should:

- Not rely on the sole contractual commitments made by the app providers to collect valid consent, but rather provide for concrete and precise obligations as to how the consent should be obtained from data users (*e.g.*, by agreeing on a banner template to be displayed at the installation of the app)
- Control if such banner template is actually displayed in practice, if necessary by carrying out an audit
- Provide users with complete and clear information (including the name of the data controller) at the installation of the app, before the collection process actually begins

- Enable users to choose the different purposes of processing at the first layer (and not only via the preferences page, in the app settings)

Broader Implications

The GDPR's more detailed requirements for valid consent are impacting businesses at all levels of the adtech value chain. Companies with processing activities that are at least one step removed from the end user have been particularly affected.

The cases brought in France highlight the compliance challenges that these businesses face. The €50 million fine issued by the CNIL against Google two months ago confirms that businesses relying on targeted advertising for revenue generation will likely remain targets for data protection authorities' investigations and enforcement actions.

The adtech industry will also soon be the affected by the upcoming ePrivacy Regulation and the likely alignment of the regulation's fining scale with that of the GDPR. In this respect, the European Data Protection Board (EDPB) very recently released a public statement, urging the policymakers to expedite the implementation of the ePrivacy Regulation and reiterating the need for providing additional strong guarantees for all types of electronic communications.

In the meantime, national rules implementing the ePrivacy Directive still apply. The EDPB recently claimed in a 12 March 2019 opinion that data processing activities, such as the use of cookies for behavioral advertising, can trigger both the material scope of the GDPR and the ePrivacy Directive. The EDPB stated that an infringement of the GDPR might also constitute an infringement of national e-privacy rules. In such circumstances, if national law designates the data protection authority as competent authority under the ePrivacy Directive, this data protection authority has the competence to directly enforce national e-privacy rules in addition to the GDPR. On the other hand, if the data protection authority is not competent to enforce e-privacy rules under national laws, the mere fact that a subset of a processing falls within the scope of the ePrivacy Directive does not limit the data protection authority's competence to enforce under the GDPR.

Further, it is worth noting that the GDPR might have changed the standard for consent under existing national e-privacy rules, including for the use of cookies. On 21 March 2019, the Advocate General applied the GDPR requirements in the Planet49 case (C-673/17) to cookies consent declarations and stated that pre-ticked boxes cannot be used to seek such consent.

Latham will continue to monitor and report back on developments related to the GDPR and the ePrivacy Regulation.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Myria Saarinen
myria.saarinen@lw.com
+33.1.4062.2000
Paris

Elise Auvray
elise.auvray@lw.com
+33.1.40.62.20.48
Paris

You Might Also Be Interested In

French Data Protection Authority Issues €50 Million Fine in Landmark GDPR Case

The Technology, Media and Telecommunications Review — France

Data Protection in France: An Overview

France Enacts Sweeping New Data Protection Law

Endnotes

1 An IAB framework designed to "help all parties in the digital advertising chain ensure that they comply with the EU's General Data Protection Regulation and ePrivacy Directive when processing personal data or accessing and/or storing information on a user's device, such as cookies, advertising identifiers, device identifiers and other tracking technologies." For more information, see: https://www.iabeurope.eu/category/policy/tcf-updates/.

2 https://www.iabeurope.eu/policy/the-cnils-vectaury-decision-and-the-iab-europe-transparency-consent-framework/.