THE CAPITOL FORUM Vol. 6 No. 220 June 4, 2018

The Trade Desk: GDPR User Consent Difficulties Threaten Company's Data Warehousing Business

Company Update

In the days before, and after, the EU's General Data Protection Regulation (GDPR) became enforceable, many companies were, and are, scrambling to update their data collection practices to become compliant. The Trade Desk (TTD) does not appear to be one of those companies. On an investor call on May 10, CEO Jeff Green said that in his view, the GDPR would not bring about any significant changes to TTD's business.

Our analysis, however, suggests that while the GDPR may not impact some of company's business areas, the consent requirements are likely to threaten the viability of its data management businesses. In particular, TTD's growth strategy appears to be focused on growing its third-party data services, but it is precisely those types of data services that the GDPR targets.

Moreover, the GDPR goes far beyond the U.S. privacy concept of "personally identifiable information" and establishes far-reaching obligations for companies collecting and processing all types of personal data, including cookies and other tracking technologies, location information, IP addresses and online identifiers.

As discussed below, TTD's demand-side platform services could be offered on the basis of first-party data alone. On the other hand, the company's data management platform - like all data management platforms - will face difficulties in acquiring GDPR-compliant data. TTD did not respond to a request for comment for this article.

The difficulties for DMPs lie in that they require third-party data for their business, but as we have reported previously, they "currently lack a way to validate how their data providers get consent," nor do they have the possibility of reaching out to the user to request that consent. DMPs, said one expert, will therefore be "most dramatically affected" by the GDPR.

In-depth: TTD's Programmatic Advertising Business

TTD collects and processes personal data regulated by the GDPR. TTD is a demand-side and data management platform that allows advertisers to buy ads across different devices, including computers, mobile and connected TVs. The platform allows advertisers to use their own first-party data to create audience profiles.

At the same time, it uses its own data stores "to build predictive models around user characteristics, such as demographic, purchase intent or interest data," according to the company's 2017 annual report. TTD's platform is integrated with "over 135 third-party data vendors whose products we make available for purchase through our platform."

While Green said the company does not collect personally identifiable information "like names of social security numbers information," the GDPR's definition of personal data is broader than the concept of personally identifiable information.

As PageFair's Johnny Ryan said in an interview with *The Capitol Forum*, "the first thing to clarify is that in the United States, often tech companies refer to PII, that's personally identifiable information. But [the GDPR and

ePrivacy Regulation] go far beyond PII because they refer to what's called personal data. Now personal data is any information that relates to an identifiable person, whether that is direct or indirect."

Importantly, IP addresses, cookie identifiers, and other device identifiers, such as those used by TTD in its programmatic services, fall squarely within the GDPR's scope. As we have written before, moreover, "Although pseudonymizing data relaxes some requirements for companies processing the data, it does not reduce the consent obligations under the GDPR."

TTD is both a controller and a processor under the GDPR. Although Green stated that the GDPR mainly requires "publishers to be more explicit about the quid pro quo of the internet, which is that you share data and see relevant ads in exchange for free services," the activities of TTD also fall within the remit of the GDPR because it is both a data controller and a data processor.

As a DSP and a DMP, TTD both allows clients to upload their own data and to purchase access to third-party data. In its DSP functions, TTD is likely to be considered a processor under the GDPR; as part of that role, it will have to ensure that the data it uses has been obtained in a GDPR-compliant manner.

In its DMP functions, however, TTD acts as a controller under the GDPR because it is processing third-party cookie data to, for example, create lookalike audiences. As part of its controller role, TTD will need to ensure it complies with the GDPR by asking users for consent before tracking them.

Under the GDPR, companies that act as controllers are required to get opt-in consent to collect and process personal data. Although the GDPR requires companies to have opt-in consent, getting consent from users is likely going to be a difficult task for controllers acting in the ad tech background.

A company like TTD will need to rely on the front-facing websites to ask users for consent when the data is used for purposes other than granting the service. If users do not grant that consent for the website to share their data for marketing purposes, publishers will not be able to pass on personal data to companies like TTD.

Thus, Green is right in that publishers will likely be responsible for obtaining consent from users. Publishers, however, will not be able to force users to provide that consent and they will not be able to require users to provide consent in exchange for accessing a website or service.

A GDPR-compliant consent request should include a list of all the companies with which a publisher shares information, as well as an option for granting or refusing consent for each company (for an example of a GDPR-compliant consent request, see the French data protection authority's consent request here).

Ultimately, a user may feel comfortable granting a trusted publisher access to data but may decide it does not want the publisher to pass that data on to a company in the ad tech background. Indeed, the GDPR has a bias that benefits companies that have a direct relationship with the consumers. Tim Hanlon, founder and CEO of media consultancy The Vertere Group, told *The Capitol Forum* that one consequence of the GDPR is "more of an emphasis on first-party relationships between consumers and content."

TTD's DMP business relies on third-party data that is unlikely to have been acquired in a GDPR-compliant manner. On the investor call, Green dismissed GDPR concerns, stating that "In order to believe there is going to

be some massive dry up of third-party data, you have to believe that quid pro quo [users receiving free services and content in exchange for data] is under threat."
The view that the business model of services paid for with personal data is not under threat by the GDPR, however, ignores the current view of data protection authorities in Europe. As the European Data Protection Supervisor, Giovanni Buttarelli recently wrote:

"The digital information ecosystem farms people for their attention, ideas and data in exchange for so called 'free' services. Unlike their analogue equivalents, these sweatshops of the connected world extract more than one's labour, and while clocking into the online factory is effortless it is often impossible to clock off."

Buttarelli also described the take-it-or-leave-it approach as a "manipulative approach" and noted that "We and other DPAs are therefore worried that even the biggest companies may not yet understand that with the GDPR these manipulative approaches must change."

TTD's view that the GDPR does not take aim at the "free" services on the internet is also at odds with the guidance issued by the Article 29 Working Party. The Article 29 Working Party – which on May 25 became the European Data Protection Board and which is in charge of resolving conflicts in interpretation of the GDPR – has issued guidance which addresses the data collection by internet services.

In the guidance, the A29WP explains that consent is not freely given if it is a prerequisite to access a service that does not need the data for purposes of providing the service (the example provided involves a photo editing app that asks for location information that is used for behavioral advertising, but that is not needed for providing the service).

That said, TTD's DSP services may be somewhat more insulated from GDPR risk than its DMP services because they can be offered on the basis of first-party data alone. Hanlon said although GDPR is a "threat to the [ad tech] ecosystem," companies that offer more tech-oriented solutions – such as TTD's DSP – are more likely able to evolve to become GDPR-compliant. On the other hand, DMPs, which are often "third-party data repositories," will be "most dramatically affected" by the GDPR's requirements because "this is where some of the most specious actors live."

It is unclear, however, to what extent TTD is going to focus on first-party data, rather than relying on growing its business on the basis of third-party data. In its annual report, it states that its long-term growth strategy includes "invest[ing] resources in growing our data offerings, both from third-party providers as well as our proprietary data." As noted above, however, companies face GDPR risk if they have not acquired their data from GDPR-compliant sources. The greater the number of outside data sources, the greater the GDPR risk.

Moreover, even TTD's own first-party data collection may not be currently GDPR-compliant: TTD stated in its annual report that "We also allow consumers to opt out from the use of data we collect for the delivery of targeted advertising." The GDPR, however, requires opt-in, rather than opt-out consent. If all of its current proprietary data has been collected on the basis of opt-out consent, then it is not GDPR-compliant.

Article 82 of the GDPR is also a source risk for TTD. Regardless of whether the company is acting as a DSP or DMP, however, it is still liable for GDPR violations if it processes data that was not acquired in a GDPR-worthy manner.

Simon McGarr, a data protection consultant with Data Compliance Europe and a practicing solicitor, told *The Capitol Forum*, the GDPR provides for a number of enforcement methods in addition to the fines, including "supply chain enforcement methods," so that "entities who are dealing with data now are liable for their processors, the people they pass the data onto." As Article 82 of the GDPR states, in cases of multiple controllers and processors, "each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject."

Although TTD's top executives may see the GDPR as a piece of legislation affecting publishers rather than ad tech companies, the activities of most ad tech companies fall squarely within its purview. Ignoring the requirements of the GDPR, therefore, is not something companies responsible for collecting and processing European residents' personal data can likely afford to do without the possibility of an enforcement backlash.