Bloomberg Law®

Privacy and Security Law Report®

INSIGHT: A Canary in the Ad Tech Coal Mine? German DPAs Announce Opt-In Regime for Online Advertising

Data Protection

Daniel Felz and Peter Swire of Alston & Bird summarize how the EU's ePrivacy Directive introduced consent requirements for online user tracking and profiling; focus on German data protection authorities' assertion that Germany's opt-out regime no longer applies; and evaluate what that may mean for ad tech stakeholders going forward.

BY DANIEL FELZ AND PETER SWIRE

Prior to the entry of the General Data Protection Regulation, German practice permitted online and mobile tracking, analytics, and profiling for marketing purposes on an opt-out basis, provided that certain internal privacy safeguards were implemented. However, on April 26, the coalition of German data protection authorities published a position paper stating that as a result of the GDPR, tracking, analytics, and profiling for marketing purposes is now subject to an opt-in regime.

Daniel Felz is an attorney with Alston & Bird in Dallas and a former assistant professor of law in Germany, and Peter Swire is a senior counsel at Alston & Bird in Atlanta and the Elizabeth & Tommy Holder Chair of Law and Ethics at the Scheller College of Business at Georgia Institute of Technology. Both are members of the firm's privacy and data security team.

The paper raises questions as to how websites and mobile apps can conduct generally used analytics, and employ tracking technology and maintain information on their users. Additionally, it potentially affects how the larger ad tech environment will function in Germany under the GDPR.

This article provides a brief summary of Germany's law of online tracking, then evaluates the German DPAs' recent position paper. It begins by summarizing how the EU's ePrivacy Directive introduced consent requirements for online user tracking and profiling, and how Germany implemented these via an opt-out regime. It then focuses on the German DPAs' assertion that Germany's opt-out regime no longer applies, and on the responses this assertion has garnered from practitioners and industry associations. The article closes by evaluating what the German DPAs' action may mean more generally for ad tech stakeholders going forward.

 ISSN 1538-3423

The ePrivacy Directive and Its Implementation in Germany

The new DPA guidance is made under the current ePrivacy Directive. Although the EU is considering revising the ePrivacy Directive into a new ePrivacy Regulation, the DPA guidance is intended to apply immediately.

1. The ePrivacy Directive. The EU passed the ePrivacy Directive in 2002 to provide harmonized rules for a number of digital technologies and communications services. The EU updated the ePrivacy Directive in 2009 by passing amending legislation sometimes referred to as the ''Cookie Directive.'' This amendment resulted in the current form of Article 5(3) ePrivacy Directive, which states in relevant part: ″[T]he 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 . . . about the purposes of the processing.''

2. Germany's Implementation of Article 5(3) ePrivacy Directive. When the current version of Article 5(3) ePrivacy Directive entered into force in 2009, EU member states were given until May 25, 2011, to pass legislation implementing it into their national law. Germany, however, never passed subsequent implementing legislation.

Instead, two years prior to the Cookie Directive, in 2007, Germany passed the Telemedia Act (TMG), and the German government took the position that the act's provisions adequately implemented the requirements of the 2009 amendments to Article 5(3) ePrivacy Directive. The European Commission is reported to have supported the German government's position. In contrast, the German DPAs initially stated they saw the Telemedia Act as needing updating in light of ePrivacy's new cookie rules, and later made a stronger statement describing the TMG's cookie and tracking rules as ''unacceptable.'' But the DPAs also indicated they accepted that, even if they considered it incomplete, the TMG remained Germany's statutory implementation of ePrivacy cookie and tracking rules, and that these rules could only be changed via new legislation. As a result, until now, the 2007 Telemedia Act served as Germany's implementation of the ePrivacy Directive's provisions on cookies and other tracking technologies.

3. The Telemedia Act. The Telemedia Act governs the provision of ''telemedia services'' in Germany. Telemedia services are defined broadly as all ''electronic information and communications services'' that do not fall under the separately regulated areas of telecommunications or broadcast media. Many common digital offerings thus constitute ''telemedia services'' within the meaning of the TMG — e.g., websites, mobile apps, search engines, internet fora, Over-The-Top messengers, and internet-based email. The TMG contains general rules for operating a number of digital platforms and technologies.

TMG Rules on Cookies, Analytics, and User Profiles

More pertinently, the TMG contains rules relevant to how website/app operators can collect and track user data, and use it for profiling or advertising. These rules are set forth in Chapter 4 of the TMG, which contain § § 11-15a TMG. In particular, the following provisions are relevant:

- Section 15(1) TMG permits website/app operators to collect ''usage data,'' defined as data necessary to facilitate the use of a website/app, or to bill users. The TMG identifies the following as ''usage data'':
  - factors for identifying the user;
  - information about the beginning, end, and scope of the user's usage of the website/app; and
  - information about the telemedia services used by the user.

  This is not understood as an exhaustive list, and indicates that the kind of information often obtained via cookies, beacons, and other tracking technology (e.g., in-site clickstream data, session data, etc.) can often be considered ''usage data.''
- § 15(3) TMG permits websites/apps to use the above-referenced usage data ''to create usage profiles for purposes of advertising, market research or for tailoring the design of the [website/app] in a needs-based manner.'' For this, the TMG does not require prior opt-in consent. Instead, the website/app operator, to create and use such user profiles, must:
  - use only pseudonymous or anonymous data to conduct analytics or create profiles;
  - store analytics/profile data separately from data that directly identifies users; and
  - provide users with an opt-out of analytics and/or profiling and reference it in the website/app privacy notice.
- As for informing users of analytics, profiling, and online advertising, § 13(1) TMG requires website/app operators to ''inform the user at the beginning of the session about the nature, scope, and purposes for which personal data are collected and used.''

As a result of the foregoing provisions, German practice for years conducted web-based use of tracking technologies, as well as the associated analytics and profiling for marketing purposes, on an opt-out basis. It was not uncommon, as late as 2016, to find major German websites complying with the TMG by simply placing a link to a privacy notice at the bottom of their web pages, and using that notice to describe their tracking, analytics, and online advertising practices. More recently, German websites have begun to add cookie banners. Comparatively few major German websites have used a 'cookie layer' that required click-through to access a website. A May 2018 study identified major German publishers that were, without requiring users to give prior consent, placing more than 40 cookies on user devices for tracking, analytics, and marketing purposes.

Parallel Article 29 Working Party Guidance on Cookies, Online Advertising

The TMG's opt-out approach differed from guidance that, during the same time period, the Article 29 Working Party (WP29) developed for tracking technologies and online advertising.

- In 2010, WP29 provided an opinion on online behavioral advertising (OBA) which required opt-in consent for the placement of cookies or other tracking tech-

nology — i.e., ''consent must be obtained before the cookie is placed and/or information stored in the user's terminal equipment is collected, which is usually referred to as prior consent.'' WP29 based this opt-in approach largely on Article 5(3) ePrivacy Directive language requiring that users ''have given his or her consent, having been provided with clear and comprehensive information'' about cookies. WP29 further indicated that browser settings should not be seen as a valid means for obtaining user consent.

■ Following this opinion, the Internet Advertising Bureau (IAB) proposed a best practice recommendation for OBA, which it presented to WP29. The IAB proposed placing an advertising icon on online ads, which users could click to opt out of personalized advertising. WP29 reviewed the recommendation and opined that it ''does not result in compliance with'' Article 5(3) ePrivacy Directive, suggesting that only a limited subset of cookies could be placed without prior consent. WP29 also noted that ''national regulators are ultimately responsible for assessing legal compliance of the OBA providers.''

■ WP29 subsequently clarified in a more detailed opinion that certain session cookies, generally placed by first-party publishers, did not require consent when they were necessary for authentication or for providing user-requested functionalities such as shopping carts or Flash videos. But it continued to indicate that prior opt-ins should be obtained for third-party cookies used in analytics or advertising.

■ WP29 again provided cookie consent guidance in 2013. Perhaps responding to emerging differences in consent standards among EU member states, WP29 addressed whether a user's continued use of a website without clicking a cookie banner could constitute valid consent. WP29 indicated that merely ''stay[ing] on the entry page without any further active behavior'' would not constitute consent. Instead, information about cookies had to be clearly presented to users (e.g., through a cookie banner), and consent could only be presumed when, in light of the information presented, the user's use of the website could reasonably amount to an indication of ''his wishes.''

Thus, the WP29 guidance generally suggested that Article 5(3) ePrivacy Directive should be interpreted as requiring an opt-in regime for the use of cookies and tracking technology in the context of advertising-related analytics and profiling. This interpretation differed from the opt-out regime, outlined above, that Germany's TMG permitted to implement the same Article 5(3) ePrivacy Directive requirements.

The German DPAs' Guidance

Although the TMG's approach may have differed from WP29's guidance, the TMG remained the law in Germany, and German practice generally followed the TMG's opt-out approach. However, on April 26, the German Datenschutzkonferenz (DSK) issued a position paper stating that the TMG no longer applies under the GDPR, and that as a result, all web-based analytics, tracking, and profiling require opt-in consent. The DSK is an association of the German DPAs, including the 16 state-run DPAs (which have general jurisdiction over private companies) and Germany's federal DPA (which has limited jurisdiction over telecommunications and postal services companies). Its position paper can be taken to represent the general opinion of the German DPAs.

The DSK provided a nine-point argument as to why the TMG is no longer effective law, and why an opt-in regime for tracking technologies should apply in Germany. Summarized, the DSK's argument is as follows:

■ The TMG's Chapter 4, which contains the provisions permitting user tracking and profiling on an opt-out basis, is actually not an implementation of the ePrivacy Directive but of the Data Protection Directive. It is thus replaced by the GDPR, since the GDPR replaces all existing implementations of the Data Protection Directive.

■ Thus, § § 13, 15 TMG are no longer effective law, and thus cannot be used as a basis for conducting internet-based analytics, tracking, or profiling. At the same time, Article 5(3) ePrivacy Directive cannot apply directly within Germany because, as an EU directive, it has no direct effect.

■ There is thus no 'live' legal provision implementing Article 5(3) ePrivacy Directive in Germany. Instead, the legality of internet-based tracking, profiling, analytics, and advertising must be evaluated solely on the basis of the GDPR.

■ As a result of applying the GDPR:

  ■ Companies can rely on their legitimate interests only for ''processing that is absolutely necessary . . . to provide the service requested by the data subject,'' or for limited ''additional processing'' a case-by-case balancing of interests shows to be permissible.

  ■ But ''prior consent is required'' in all cases where websites or apps use ''tracking mechanisms that make data subjects' Internet activity traceable'' or ''create user profiles.'' GDPR-style unambiguous consent must be obtained ''before cookies are placed and/or information stored on users' terminal devices are collected.''

■ Requiring this kind of opt-in under the GDPR ''is consistent with the European understanding of Article 5(3) of the ePrivacy Directive.'' In the DSK's words, ''in the majority of EU Member States, the ePrivacy Directive has been fully transposed into national law or the supervisory authorities already require an 'opt-in' corresponding to Article 5(3) of the ePrivacy Directive.''

Notably, the above analysis and proposed opt-in regime apply only to private data controllers, such as companies. The DSK does not apply it to public or governmental entities.

Responses to the DSK's Position Paper

The DSK's position paper represents a significant change in Germany's legal framework for online tracking, profiles, analytics, and advertising. As a result, a number of responses have been published. Most criticisms arise from practitioners and associations representing digital marketing or ad tech participants. Among the more salient critiques that have been raised include:

■ **The GDPR does not replace the TMG.** Several industry associations dispute the DSK's claim that the GDPR has rendered the TMG ineffective. In a public comment, the German Association for IT, Telecommunications, and New Media (BitKom) argues that the DSK ''sweepingly declares'' that all TMG tracking provisions are inapplicable under the GDPR, even though

only ''a portion'' of the TMG was designed to implement the Data Protection Directive. In contrast, BitKom argues that both Germany's federal government and the EU Commission viewed the TMG as ePrivacy implementation, and that ''in particular'' the TMG's opt-out regime ''was always viewed by the government as a sufficient implementation'' of ePrivacy cookie rules. BitKom suggests that the German DPAs are ignoring legislative will to obtain a desired outcome. BitKom indicates it represents over 2,500 ''companies of the digital economy'' in Germany.

■ **If the DSK is exclusively applying the GDPR to evaluate the legality of tracking, it should not read ePrivacy provisions into the GDPR.** The German Advertising Federation argues the DSK is being inconsistent by stating that only the GDPR may be used to evaluate the legality of online tracking and advertising, then taking the position that the 'European understanding of Article 5(3) ePrivacy Directive' is what the GDPR requires. In its own words, ''[t]o justify its consent requirements, [the DSK's] position paper refers to a 'European interpretation of Art. 5(3) of the ePrivacy Directive' ''; but that ''as regards telemedia services processing personal data, the ePrivacy Directive is not a *lex specialis* to the GDPR, nor does it determine how the GDPR should be interpreted.''

■ **The GDPR expressly anticipates that profiling will be conducted on the basis of legitimate interests.** A number of practitioners point to GDPR provisions that permit profiling, and foresee opt-outs from marketing-related profiling, as indications that the GDPR permits online tracking and profiling without prior consent. As an example, one German attorney identifies ''GDPR Recital 47, which expressly names direct marketing as a potential legitimate interest,'' as well as ''Art. 21(1) GDPR, which provides an opt-out right for profiling associated with marketing,'' as ''clear arguments that tracking and targeting — depending on their 'invasiveness' and reasonable expectability — can be based on legitimate interests.'' Another German attorney argues that Recital 47 and Art. 21(1) GPDR ''would not be needed if the creation of every profile required consent.''

■ **The DSK's position is overbroad.** To quote one practitioner, ''[u]nder the DSK's [position paper], every personalized link in an email is forbidden because it is associated with a user profile. Similarly, recognizing users returning to a website would only be permissible with express consent of the users, because it uses a (pseudonymous) user profile.''

■ **Pervasive consent requirements potentially undermine data minimization because they require identifying individuals for consent purposes that ad tech players would rather keep pseudonymous.** The German Association for the Digital Economy argues that requiring consent that can be tied to users potentially runs contrary to data minimization principles. ''Where companies neither know nor can effectively know the identity of individual persons, they should be permitted to limit themselves to processes that process less data in secure environments,'' it says.

■ **It sends a questionable message to apply an opt-in requirement for tracking only to private controllers, but not public controllers.**

■ **The DSK's default requirement of opt-in consent is arguably inconsistent with the ECJ's Breyer decision.** In *Breyer v. Bundesrepublik Deutschland*, Case C-582/14, paras. 55-64 (E.C.J. Oct. 19, 2016), the ECJ evaluated whether Germany's TMG could be interpreted as limiting controllers' ability to collect and use telemedia usage data ''only to the extent that is necessary to facilitate and charge for the specific use of online media by the user,'' and as requiring consent for any other uses. In *Breyer*, the German government operated websites that logged IP addresses to detect and prevent cyberattacks; these websites were subject to the TMG. Before the case was referred to the ECJ, a German appeals court interpreted the TMG as only permitting user data to be stored beyond the end of a session for billing purposes, and as not permitting companies' legitimate interests to serve as a basis for any further storage or uses. Instead, user consent was required. On review, the ECJ held that the Data Protection Directive's Article 7(f) (the predecessor norm to Art. 6(1)(f) GDPR) expressly permitted controllers to process data on the basis of legitimate interests. As a result, member states could not ''exclud[e], categorically and in general, the possibility of processing certain categories of personal data'' on the basis of companies' legitimate interests. Legislation to the contrary would be ''preclude[d].'' On remand, the German Supreme Court held that the § 15 TMG permitted user data to be processed on the basis of legitimate interests.

■ **Requiring consent for all tracking and profiles — even if pseudonymous — disregards the GDPR's risk-based approach and encouragement of pseudonymization.**The German Advertising Federation further argues that ''when specific data processing scenarios should be permitted only on the basis of consent, the GDPR expressly names them,'' such as in the case of sensitive data.

Evaluation and Conclusion: A Canary in the Coal Mine?

The volume of responses to the DSK's position paper indicate that the DSK's position is seen as a significant shift in German law. Perhaps in response, just over month after publishing its position paper, the DSK announced it was opening a period of public comment. The German DPAs invite all stakeholders to provide responsive comments ''via their trade associations and representatives,'' in particular regarding questions on ''practical execution.'' Companies can submit comments until June 29.

In the meantime, market participants have engaged German DPAs for further guidance on the DSK's position paper. The German DPAs appear to be responding to inquiries in an ad hoc manner; thus far, no further guidance has issued from the DSK. As an example, one consultancy states that it contacted the DPA of North Rhine-Westphalia for further guidance as to what cookies placed by publishers require prior consent. According to it, the DPA responded that:

■ session cookies do not require consent;

■ analytics cookies and trackers provided by Piwik/Matomo can be used on an opt-out basis if user data is pseudonymized and stored locally; but

■ Google Analytics or ''other third party analytics tools'' can only be used with prior consent because user data is transferred to third parties who can use them to enhance their own complex profiles of users' online activity.

At present, the discussion appears to be at a nascent stage. The German DPAs' focus appears to be on publishers and common third-party analytics or tracking technologies that they integrate into their websites or apps. There has been little mention of the wider ad tech environment, such as agencies, supply- or demand-side platforms, exchanges, or networks. As one example, the German Association for the Digital Economy obliquely suggests the complexity of the ad tech world in arguing that, ''in light of current market conditions,'' strict consent requirements for information society services are not likely to improve user protection, since click-through consent results in users consenting to ''all possible processing activities.'' Instead, ''clearly regulated statutory permissions'' that set forth ''targeted requirements of the processes and technologies in use'' would create better protections.

Despite this, ad tech participants could consider viewing the DSK's position paper as an early indicator of the attitude that DPAs in the post-GDPR world may take toward online advertising. For years, WP29 has promoted the position that third-party tracking technology, and any third-party-driven analytics or advertising associated with it, require prior opt-in consent from website or app users. This stood in contrast to WP29's position toward session cookies used for security, authentication, or user-requested functionalities (which WP29 held did not require consent), and first-party analytics (which WP29 indicated resulted in a low privacy risk). On the whole, WP29's positions could be interpreted as reflective of an attitude disfavoring online advertising technology within the broader DPA community. Like WP29, the DSK is composed entirely of DPAs. Its effort to establish an opt-in regime in Germany may be its signaling that this attitude persists in the post-GDPR world and that, in the absence of EU legislation to the contrary, DPAs will attempt to use GDPR consent rules and their enhanced enforcement powers to alter online advertising practices.

German DPAs' positions may develop increased influence within the EU in light of the GDPR and the forthcoming ePrivacy Regulation. Prior to these statutes, internet consent rules were a matter of local law, implementing a directive and not a regulation; Germany had its statute implementing the ePrivacy Directive, as did the Netherlands, Italy, Ireland, etc. These statutes could differ significantly, and DPA action in one member state did not necessarily affect how other member states interpreted their own statutes. Now, however, the EU is moving toward harmonizing data protection and ePrivacy law via the GDPR and ePrivacy Regulation. A German interpretation of GDPR and/or ePrivacy rules is thus no longer a strictly local matter, but instead potentially persuasive authority in a larger European discussion of consent requirements. While it remains to be seen whether other DPAs or courts follow the German DPAs' position on consent requirements, German DPAs now have a basis for attempting to drive European standards.

While DPAs' efforts may primarily focus on publishers at present, modifications to publisher practices are likely to flow through the ad supply chain. The debates on the forthcoming ePrivacy Regulation will show whether European lawmakers agree that consent rules should be used to address online advertising practices. A recent report by the Council of the EU indicated that lawmakers are discussing:

- (a) ''situations when consent is not necessary;''
- (b) ''making access to websites conditional on the consent to store cookies;'' and
- (c) rules for default browser settings, which could indicate a debate over whether browser settings can be considered valid indications of user consent.

To the extent that the ePrivacy Regulation leaves room for interpretation of legal requirements in the online advertising context, it should be noted that German DPA interpretations of EU statutes — including the DSK's recent position paper — do not rise to the level of binding case law. When DPAs issue a ruling against a company, their determinations of law can be challenged before German courts, where they are subject to what amounts to *de novo* review. In practice, since privacy litigation has not been widespread in Germany, German DPAs tend to make the ''working law'' that companies follow, but it is generally recognized that courts retain the last word. This structure supports the development of case law to determine the extent and contours of the DSK's current and future positions.

By Daniel Felz and Peter Swire

Daniel Felz is an attorney with Alston & Bird in Dallas and a former assistant professor of law in Germany, and Peter Swire is a senior counsel at Alston & Bird in Atlanta and the Elizabeth & Tommy Holder Chair of Law and Ethics at the Scheller College of Business at Georgia Institute of Technology. Both are members of the firm's privacy and data security team.