I. Synopsis

The Digital Advertising Alliance’s (DAA) Self-Regulatory Principles (DAA Principles)\(^1\) cover entities\(^2\) engaged in interest-based advertising (IBA) across websites or mobile applications (apps). Companies engaged in IBA, including wireless service providers, must assess which roles they occupy under the DAA Principles and ensure that consumers are provided sufficient transparency and control in all relevant contexts. Consumers must also be provided the opportunity to consent to materially different uses of prior-collected data.

II. Company Status

T-Mobile USA, Inc. (T-Mobile) is an American wireless network operator partly owned by German telecommunications company Deutsche Telekom (DT), and based in Bellevue, Washington. T-Mobile is the second-largest wireless carrier in the United States, with 106.9 million subscribers as of the end of Q3 2021.

---

\(^1\) The DAA’s interest-based advertising principles consist of a suite of four documents: the Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles), the Self-Regulatory Principles for Multi-Site Data (MSD Principles), the Application of Self-Regulatory Principles to the Mobile Environment (Mobile Guidance) and the Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (Cross-Device Guidance) (collectively, the Principles). The full text of the Principles can be found at http://www.aboutads.info/principles.

\(^2\) The DAA Principles assign responsibilities to an entity based on its role in a particular situation. Thus, an entity can be a first party, third party, or service provider depending on the function it is performing.
III. Inquiry

This case arises from the Accountability Program’s ongoing monitoring of companies involved in IBA.

In response to publicity regarding T-Mobile’s announced changes to its Privacy Notice, the Accountability Program examined T-Mobile’s Privacy Notice as published on its website. There, it found the following text prominently displayed under the heading “What’s New”:

[S]tarting April 26, 2021, T-Mobile will begin using some data we have about you, including information we learn from your web and device usage data (like the apps installed on your device) and interactions with our products and services, for our own and 3rd party advertising, unless you tell us not to.

In addition, the Accountability Program came into possession of an email sent by T-Mobile to a T-Mobile subscriber with the subject line “Updates to Terms & Conditions and Privacy Notice.” In that email, T-Mobile stated, inter alia:

We wanted to tell you about an update to our Privacy Notice effective February 23, 2021. . . . Like many companies, we will share select data that doesn’t directly identify you to make advertising more useful to you. . . .

- If you prefer not to have your data used to increase advertising relevance, you can opt-out at any time.
- Starting April 26th, T-Mobile and 3rd parties may provide more relevant advertising by using broadband and other usage information, unless you opt-out.
- You can change your settings at any time.

In reviewing T-Mobile’s Privacy Policy, the Accountability Program found that it stated:

We keep this privacy notice up to date. When we make changes, we will let you know by updating the date at the top of the page. If we’re making a big change (one that is considered material), we’ll also

---


5 Id.

6 E-mail from T-Mobile, news@t-mobile-email.com (Mar. 5, 2021) (on file).
reach out to you (e.g., by text or email or with your bill). If you keep
using our products and services after we notify you of a big change,
we’ll take that to mean you’re fine with it.7

Based on this phrasing, the extent to which relevant portions of T-Mobile’s privacy
notices did not appear to be clear or prominent, and the changes to T-Mobile’s
policies, the Accountability Program became concerned that T-Mobile’s policies
might not be compliant with the OBA Principles and the Mobile Guidance.

IV. Issues Raised

A. Material changes to IBA practices

Under the OBA Principles, “Entities should obtain Consent before applying any
material change to their Online Behavioral Advertising data collection and use
policies and practices prior to such material change. A change that results in less
collection or use of data would not be ‘material’ for purposes of this Principle.”8 In
other words:

a company must obtain opt-in consent if (1) it makes a material
change to its IBA practices resulting in more expansive uses of data
than previously disclosed to the user, and (2) the company applies
this material change retroactively to data previously collected from
the user under an earlier version of its privacy policy.9

If both prongs of this two-part test are satisfied, a covered entity is required to obtain
user Consent prior to its use of previously collected data.

One situation where this Principle directly applies is when a company collects data
for IBA and has a provision in its privacy disclosures stating that the company
reserves the right to expand its use of such previously collected data in the future. In
re IQM Corporation provides an example of this situation.10

In that case, the company’s privacy policy stated that “[u]se of information we collect
is subject to the Privacy Policy in effect at the time such information is used.”11 This
phrasing suggested that consumers would be subject to the version of the privacy
policy in effect at the time the data’s use, rather than the version of the privacy policy
at the time the data was collected, and that consumers might not be given the

---

7 T-Mobile Privacy Notice, T-MOBILE (May 5, 2021), https://www.t-mobile.com/privacy-
center/our-practices/privacy-policy.
8 OBA Principles § V; see also Commentary at 38–9.
10 No. 96-2019 (2019).
11 Id. at 3.
opportunity to consent to material changes if such changes took place between the
time a consumer’s data was collected and when it was used.\textsuperscript{12}

However, as the company stated that its business practice was \textit{not} to apply material
changes to IBA activity retroactively to previously collected data, it amended its
privacy disclosures to clarify the issue for consumers.\textsuperscript{13} These actions resolved the
company’s compliance issues regarding material changes to IBA usage.\textsuperscript{14}

Similarly, in \textit{In re Ledbury Inc.}, the company’s disclosures stated: “We reserve the
right to change our Privacy Policy and our Terms of Use at any time. . . If we make
material changes to this policy, we will notify you here, by email, or through notice
on our home page.”\textsuperscript{15} Because this language did not specify whether Ledbury would
apply future material changes retroactively to data previously collected under earlier
versions of its privacy policy, the resulting ambiguity raised a possible compliance
issue under the Material Changes provision of the OBA Principles.\textsuperscript{16} To resolve this
issue, the company amended its privacy disclosures to clarify its practices: that it
would \textit{not} apply material changes to its IBA activity retroactively to previously
collected data without giving the user choices regarding these changes.\textsuperscript{17}

Likewise, in \textit{In re Kargo Global, Inc.}, language in the company’s privacy policy
implied that a user might not be provided the opportunity to consent to material
changes to the privacy policy if such changes took place between the time the user’s
data was initially collected and the time it was used, raising a possible compliance
issue with \textit{OBA Principles} § V.\textsuperscript{18} As the company’s actual practices were to \textit{not} apply
material changes retroactively regarding previously collected data for IBA, the
company remedied its § V compliance issues by altering its privacy disclosures
accordingly.\textsuperscript{19}

\textbf{B. Service Provider Responsibilities}

Under the \textit{OBA Principles}, “Service Providers should not collect and use data for
[IBA] purposes without Consent.”\textsuperscript{20} An entity is a Service Provider:

\begin{itemize}
\item \textsuperscript{12} \textit{Id.} at 3–4.
\item \textsuperscript{13} \textit{Id.} at 11.
\item \textsuperscript{14} Id.
\item \textsuperscript{15} \textit{In re Ledbury Inc.}, No. 87-2018, at 2–3 (2018).
\item \textsuperscript{16} \textit{Id.} at 3.
\item \textsuperscript{17} \textit{Id.} at 4–5.
\item \textsuperscript{18} No. 97-2019, at 4 (2019).
\item \textsuperscript{19} \textit{Id.} at 7–8.
\item \textsuperscript{20} \textit{OBA Principles} § III.A.B.1.
\end{itemize}
to the extent that it collects and uses data from all or substantially all URLs traversed by a web browser across Web sites for [IBA] in the course of the entity's activities as a provider of Internet access service, a toolbar, an Internet browser, or comparable desktop application or client software and not for its other applications and activities.21

In the case of a company that provides wireless internet access, then, the conduct that would qualify an entity as a Service Provider under the OBA Principles is:

i. The collection of data (i.e., information) from all or substantially all URLs traversed by a browser across websites;

ii. in the course of the company's activities as an ISP, and not for other activities;

iii. which is then used for IBA, not for other applications.

C. First Party Responsibilities

Under the Mobile Guidance, “[a] First Party is the entity that is the owner of an application, or has Control over the application, with which the consumer interacts, and its Affiliates.”22 First parties that authorize a third party to collect or use Cross-App Data for IBA must “provide a clear, meaningful, and prominent link”—that is, enhanced notice—to a disclosure (or “notice”) that “(1) describes the third-party collection, (2) points to a choice mechanism/setting or lists all third parties with links to their opt outs, and (3) contains a statement of adherence to the DAA Principles.”23 This enhanced notice “must be provided prior to download (e.g., in the app store on the application’s page), during download, on first opening of the app, or at the time cross-app data is first collected, and in the application’s settings or any privacy policy.”24

D. Third Party Responsibilities

Under the Mobile Guidance, “[a]n entity is a Third Party to the extent that it collects Cross-App Data or Precise Location Data from or through a non-Affiliate’s application, or collects Personal Directory Data from a device.”25

21 Id., Definition I at 11.
22 Mobile Guidance § I.G; cf. OBA Principles, Definition F at 10 (“A First Party is the entity that is the owner of the Web site or has Control over the Web site with which the consumer interacts and its Affiliates.”).
24 Id. at 4–5.
25 Mobile Guidance § I.N; cf. OBA Principles, Definition J at 11 (“An entity is a Third Party to the extent that it engages in Online Behavioral Advertising on a non-Affiliate’s Web site.”).
1. Third Party Notice Requirement

Under the Mobile Guidance,

third parties who engage in the collection or use of cross-app data for IBA must provide a clear, meaningful, and prominent notice on their websites or accessible from the applications that host them. This notice must include (1) the types of data collected, (2) the uses of such data, (3) an easy-to-use mechanism for exercising choice with respect to the collection and use of such data or the transfer of such data to a non-affiliate for IBA, and (4) the fact the third party adheres to the DAA Principles.26

V. Analysis and Company Response

In response to the Accountability Program’s inquiry letter, T-Mobile immediately conducted a comprehensive review of its compliance with the DAA Principles to identify any areas in its compliance protocols that needed strengthening. The company worked diligently to find comprehensive solutions to each issue and consulted with the Accountability Program on its plan to come into compliance with the DAA Principles, as explained below.

A. Material Changes to IBA Practices

1. T-Mobile’s current IBA Program

In its representations to the Accountability Program, T-Mobile indicated that its IBA program, which began in April 2021, would be collecting and using data for the purposes of IBA, in cases where it had not previously done so, and which had not been disclosed in previous versions of its privacy policy. This was a material change to T-Mobile’s IBA practices resulting in more expansive uses of data than previously disclosed to the user, satisfying the first prong of the two-part Ledbury test, see subsection IV(A), supra.

But T-Mobile also indicated that it would not use data collected prior to the commencement of its IBA program for the purpose of IBA. Consequently, because the material change is not applied retroactively to data collected under the terms of its previous privacy disclosures, T-Mobile’s actions do not satisfy the second prong of the Ledbury test, and T-Mobile is not obliged to obtain Consent prior to its use for IBA. Consequently, the Accountability Program did not recommend any changes to T-Mobile’s practices with regard to Material Changes.

2. Future Material Changes

T-Mobile's Privacy Policy states:

We keep this privacy notice up to date. When we make changes, we will let you know by updating the notice and the date at the top of this page. In addition, prior to making a material change to how we use or share your data, we'll also reach out to you (e.g., by text or email or with your bill). If you keep using our products and services after we notify you of a big change, we'll take that to mean you're fine with it.\(^\text{27}\)

Or, to put it another way, T-Mobile is stating that if it makes material changes to its privacy notice (which could include provisions related to changes in its IBA practices), it will notify its customers and give them the opportunity to opt out, but will not seek Consent from them.\(^\text{28}\)

As in \textit{IQM}, \textit{Ledbury}, and \textit{Kargo}, this phrasing creates compliance issues, as it suggests that T-Mobile reserves the right to make material changes in the future, which could potentially include the retroactive use of previously collected data for IBA, \textit{without} collecting Consent from consumers. If T-Mobile does \textit{not} intend to not to make material changes to its IBA practices that would include the retroactive repurposing of previously collected data, the Accountability Program recommends that T-Mobile amend its privacy disclosures to clearly indicate to its customers that any material changes it may make will \textit{not} apply retroactively to previously-collected data for IBA. And if there is a possibility that T-Mobile may want to repurpose previously collected data for IBA in the future, the Accountability Program recommends that T-Mobile amend its privacy disclosures to clearly indicate that such repurposing will only occur with a customer's Consent, which is \textit{opt-in}.

3. Company Response

T-Mobile accepted the Accountability Program's recommendation to modify its privacy disclosures. The pertinent section now reads as follows:

We keep this privacy notice up to date. When we make changes, we'll let you know by updating this notice and the date at the top of this page. In addition, prior to making a material change to how we use or share your data, we'll also reach out to you (e.g., by text or email or with your bill). If you keep using our products and services after we notify you, we'll take that to mean you're fine with the changes for any new data we collect. Those changes will not apply to previously


\(^{28}\) Under the \textit{OBA Principles} and \textit{Mobile Guidance}, Consent must be affirmative, i.e., opt-in ("an individual's action in response to a clear, meaningful, and prominent notice"). \textit{Mobile Guidance} § 1.B (emphasis added).
collected personal data unless we get consent from impacted consumers.29

B. T-Mobile as a Service Provider

1. T-Mobile’s Status Under the OBA Principles

In its formal Reply, and in statements made by its staff and counsel, T-Mobile specifically disclaimed the use of data collected from web browsing for IBA. Consequently, even to the extent that it may collect data “from all or substantially all URLs” traversed by its customers’ web browsers for other purposes, because it does not use such data for IBA, it is not a “Service Provider” within the contemplation of the OBA Principles, see subsection IV(B), supra.

Although T-Mobile does not use data collected from all or substantially all URLs for IBA, and is not a “Service Provider,” T-Mobile’s disclosures as provided in its Privacy Policy and other documents appear to indicate that it does collect and use such data for IBA.30 As always, when a company claims to engage in certain data collection and use practices, we take it at its word, assume the behavior is happening, and evaluate its compliance accordingly. Further, to the extent that T-Mobile does not engage in such activity at the current time, but claims that it does, it is essentially reserving the right to do so in the future without changing its disclosures.

Consequently, the Accountability program recommends that T-Mobile revise its disclosures to make clear that T-Mobile does not engage in such activity. This would serve the purposes of better informing its customers as to the extent of its collection and use of data for IBA. It would also mean that if T-Mobile ever did collect and use web browsing data for IBA in the future, T-Mobile would be required to properly notify its customers and collect Consent prior to such collection and use.

2. Company Response

In response to the Accountability Program’s recommendation, T-Mobile removed language referring to the collection of web browsing activity from the relevant section of its privacy policy. The company further took steps to delineate the kinds of data it collects and uses for analytics as well as for IBA, thereby increasing the overall clarity of its disclosure.


C. T-Mobile as a First Party

In its disclosures to the Accountability Program, T-Mobile stated that some data, including non-Affiliate application use over time, that is used for IBA, is collected from certain T-Mobile applications. But because T-Mobile has not authorized third parties to engage in data collection directly from such apps, T-Mobile is not a First Party within the contemplation of the DAA Principles, and T-Mobile is not obliged to provide notice or enhanced notice in its role as a first party.

D. T-Mobile as a Third Party

In its statements to the Accountability Program, T-Mobile indicated that it collects and uses Cross-App Data for IBA from all or substantially all non-Affiliate applications on a device, qualifying it as a Third Party and subjecting it to the pertinent requirements of the Mobile Guidance. In this case, we focus on T-Mobile's compliance with the Third Party Notice requirement.

T-Mobile provides a number of documents in the “Privacy Center” on its website; most relevantly, these include a “Privacy Notice” and an “Advertising and Analytics” document. Of these, the Advertising and Analytics document most closely resembled the notice that the Accountability Program was looking for during its initial review of T-Mobile's disclosures. A substantially similar set of IBA disclosures are located in T-Mobile's privacy policy and are available through a jump link entitled “Your Personal Data Choices.” Both documents will be discussed at points in the following analysis.

1. Types and uses of data

The Advertising and Analytics document states under the heading “Data We Use for Advertising and Analytics”:

The type of mobile broadband, online, and device data we and others may collect and use for advertising and analytics include . . .

- Unique IDs such as device IDs, ad IDs, and cookie IDs. See article for more information about cookies and ad IDs
- Addresses of websites visited
- Types of websites visited, like sports sites, music sites, etc.

• Applications, content, and features used—including how much time you spent using them, and information from servers that host these apps, content, and features

• Information about use of products and services, such as data and calling features, device type, operating system type, and amount of use.\(^{32}\)

Further down the document, under the heading “How Your Data is Used to Target Ads,” the document states:

under T-Mobile’s personalized ads program, we use and analyze data from things like device and network diagnostic information (Android users only), apps on your device, and broadband information. . . . Using this information, we create groups known as “audience segments,” which may be used by T-Mobile or sold to third parties to make ads more relevant to you.\(^{33}\)

These statements do not comply with the requirement that Notice be “clear, meaningful, and prominent” in providing “(1) the types of data collected, (2) the uses of such data.”\(^{34}\) The first section (under “Data We Use for Advertising and Analytics”), while it enumerates specific types of data collected, does not differentiate between uses of data, lumping them under “Advertising and Analytics.” The second section (under “How Your Data is Used to Target Ads”) indicates that T-Mobile uses and analyzes “data from things like device and network diagnostic information (Android users only), apps on your device, and broadband information” for IBA.\(^{35}\) Because it does not specifically indicate which types of data are used for IBA (only that data “from things like” certain data sources are used), it leaves consumers unsure as to precisely what types of information will be used for IBA.\(^{36}\)

Because the open-ended phrasing is vague, and the lack of specific, defined uses for each category of data leaves consumers without adequate information to make an informed choice as to the use of their information, these provisions are not compliant with the requirement that Notice be “clear” and “meaningful.”

---


\(^{33}\) Id.

\(^{34}\) Vdopia at 6.


\(^{36}\) The IBA disclosure in T-Mobile’s prior privacy policy similarly muddied the distinction between data collected for analytics and advertising, leaving consumers unsure which kinds of data may be collected for which purposes.
As discussed in the immediately preceding section, T-Mobile greatly increased the clarity of its disclosures by updating, expanding, and better stratifying its IBA disclosures in its privacy policy. The updates to this section obviate the need to further update the footer notice page that was originally the focus of the Accountability Program’s analysis.

2. Mechanism for exercising choice

The Advertising and Analytics document includes both opt-out instructions for T-Mobile’s own “personalized ads” program (under the heading “How Your Data is Used to Target Ads”), and links to the DAA’s AdChoices Program (under the heading “Your AdChoices”). The text before the opt-out for T-Mobile’s “personalized ads” program includes a description of how the collected data may be used by T-Mobile for IBA or may be transferred to a third party for IBA. Putting aside any issues of prominence (discussed in subsection (d), infra), the inclusion of the choice elements on the page is sufficient to satisfy T-Mobile's obligation to provide, as part of its Third Party Notice, “an easy-to-use mechanism for exercising choice with respect to the collection and use of such data or the transfer of such data to a non-affiliate for IBA.”

3. Statement of adherence to the DAA Principles

The Advertising and Analytics document states under the heading “Your AdChoices / Ads on your mobile device, computer, or other device,” “T-Mobile and many of its advertising partners adhere to the Digital Advertising Alliance's (DAA) Self-Regulatory Principles for Online Behavioral Advertising.” Because this statement is a “clear description” of the fact that T-Mobile adheres to the DAA Principles, it is adequately compliant with the requirements of the Mobile Guidance for Third Party Notice regarding the statement of adherence. Depending on future amendments to T-Mobile's Third Party Notice, adjustment may be needed to ensure that the statement remains “clear, meaningful, and prominent.”

37 Id.
38 Id.
39 Vdopia at 6.
41 Mobile Guidance § III.A.1(d).
4. Clarity and Prominence

Under the Mobile Guidance, the requirement that Third Party Notice be “clear, meaningful, and prominent” is key.42 Burying Notice in an extensive Privacy Policy is not sufficiently prominent: as the Commentary to the Mobile Guidance makes clear, “[a]ny requirement in this guidance to provide clear, meaningful, and prominent notice would not be satisfied by providing notice hidden in lengthy terms and conditions.”43 Thus, the prominence requirement applies both to the positioning of the four required elements of Notice within the document containing such notice (particularly if Notice is provided within a longer privacy policy that addresses other issues), and to the visibility or accessibility of the document itself (as a hard-to-find document is not “prominent”).

Regarding the placement of the Third Party Notice elements with the text of the Advertising and Analytics document, the brevity of the document itself confers to the elements sufficient prominence, as little other material is included.

In terms of prominence, T-Mobile’s Advertising and Analytics document is directly linked in the footer of every T-Mobile web page with the link text “Interest-based ads.”44 This is reasonably prominent within the context of site-wide documents linked in the footer. The document is also linked to in T-Mobile’s “Privacy Center” under the “Your ads, your way” heading, where it sits in equal prominence with legally mandated disclosures and consumer controls.

T-Mobile’s disclosures are thus sufficiently prominent under the terms of the Mobile Guidance.

VI. Company statement

T-Mobile is a strong supporter of the DAA Accountability Program and the self-regulatory principles of transparency and consumer choice. We appreciate the opportunity to participate in voluntary self-regulation and are gratified by the Accountability Program’s recognition that T-Mobile is compliant with the DAA’s interest-based advertising principles.

42 Mobile Guidance § III.A.1 (“Third Parties should give clear, meaningful, and prominent notice of their Cross-App Data collection and use practices for purposes other than those set forth in Section VI.”).

43 Id. § III.A.2, Commentary, at 16; accord OBA Principles, Commentary, at 32.

VII. Disposition of decision

Practices voluntarily corrected in part, review voluntarily closed in part.\textsuperscript{45}

\textsuperscript{45} The Accountability Program also considered the issue of T-Mobile’s potential responsibility as an entity collecting or using all or substantially all Cross-App Data to obtain Consent prior to such collection or use. In light of apparent widespread lack of understanding that the Mobile Guidance requires Consent in such circumstances, and that such Consent must be demonstrated by a user’s responsive action, the Accountability Program closes its inquiry on that issue without reaching a decision. The Accountability Program is instead, as it has done in similar situations, issuing a Compliance Warning on the subject to ensure all potentially responsible parties are on notice of their obligations as of the date specified in the Compliance Warning. The Accountability Program reserves the right to reopen this inquiry with respect to that issue in the future.