

Home Depot and Meta cases: opt-in consent is needed for “secondary” online data collection and use

In two recent privacy decisions – one in Canada and the other in Europe – the groundwork has been laid for new, proactive rules regarding consent for the collection and use of individuals’ digital data.

The key finding in the federal Office of the Privacy Commissioner’s investigation into Home Depot’s tracking of customer purchase activity, and its disclosure of this information to Meta in connection with its Facebook platform, was that distinct opt-in consent for such uses was required.¹ In the absence of such opt-in, Home Depot did not obtain valid consent notwithstanding generic language in its Privacy and Security Statement that included “improving products and services” and “looking at trends and customer interests”.

A similar result was [determined by the European Data Protection Board](#) (EDPB) in the long-running case involving Meta Ireland in respect of its collection of users’ personal information for purposes of ad targeting on its Facebook and Instagram platforms. In the decision, a prominent opt-in was ruled necessary for valid consent for such collection and use, as opposed to burying disclosure of the practice in the platforms’ terms and conditions and in effect making such consent a condition of users’ using the platforms.

The underlying basis for the determinations in both cases was that consent to so-called “secondary uses” of personal information cannot be made a condition of a service for which the uses are unrelated. In essence, any consent to collection or use of such data for secondary uses must be optional for the user. This is the privacy law in both Canada under PIPEDA² and Europe under the GDPR³ – consent to collection of personal information in connection with provision of a product or service can only be required to the extent necessary to provide the service. However in Canada, in its [2009 Facebook investigation](#), the OPC had ruled that using a user’s personal information for ad targeting purposes was an integral part of the social media site’s services and in fact was necessary to support its economic model.

A similar position was taken by Meta – the new entity that now operates the Facebook and Instagram platforms – in its opposition to the complaint brought against it in the *Meta Ireland* case. Meta pointed to the “contractual necessity” provision in the GDPR as the lawful basis for its collection and use of such personal information, arguing that stipulation in the platforms’ terms and conditions of use, which users were required to accept in order to participate in the platforms, precluded the need to obtain consent.

¹ [Investigation into Home Depot Canada Inc.’s compliance with PIPEDA](#); PIPEDA Findings # 2023-001, January 26, 2023.

² [Personal Information Protection and Electronic Documents Act](#).

³ [General Data Protection Regulation](#).

While the facts of the two cases are quite distinct – Home Depot was collecting email addresses ostensibly for purposes of providing in-store customers with an e-receipt, whereas Meta through its Facebook and Instagram platforms was tracking users’ activity while using the platforms (as well as elsewhere online), the resulting – albeit evolving – principle is the same: separate, prominent opt-in consent is required for such “secondary” data collection and use.

While the OPC’s Home Depot decision has a more narrowly Canadian impact, focused on our federal and provincial privacy laws, the EDPB’s decision (if upheld on appeal) although made in the context of the GDPR, likely will have much wider impact, not the least of which that it should lead to Meta adjusting its data collection formats in all jurisdictions, worldwide. An even wider potential impact, in application of the principle beyond the Meta-specifics, is that a new, higher transparency and consent standard for online data tracking and targeting may be established.

Home Depot

Home Depot was sending in-store customers’ personal information to Meta through its Facebook “Offline Conversions” tool which allowed businesses to measure the effectiveness of their Facebook ads. Specifically, Home Depot was sending a customer’s hashed email address and their in-store purchase details to Meta when the customer provided that address, at check-out, ostensibly for purposes of providing the customer with an emailed receipt. Meta then matched the email to the customer’s Facebook account. Meta compared offline purchase information to ads delivered to the customer on Facebook, for purposes of measuring the effectiveness of those ads, and provided the results of that analysis to Home Depot in the form of an aggregated report. By using the tool, retailers such as Home Depot could send Meta in-store transaction data to: (i) understand how much of their customers’ offline activity can be attributed to ads; (ii) measure the offline return on ad spending; and (iii) reach people offline and show ads to people based on the actions they take offline.

The data sent to Meta related only to in-store customers who requested an e-receipt for their purchase. Home Depot customers were presented with an on-screen option to receive an e-receipt. If they clicked “yes”, they were then directed by the system to provide their email address. At no point in this process was reference made to Home Depot’s data sharing with Meta.

Home Depot argued that Meta was simply acting as a service provider to it in providing the report information. It stated that Meta acts as a service provider to Home Depot by “doing externally what Home Depot could have done internally”. Home Depot viewed this practice as a processing activity that did not require additional consent. However, the OPC disagreed, determining that Home Depot’s provision of such data to Meta for the purposes of measuring ad effectiveness was not within the customer’s reasonable expectations when they provided their email address for receipt purposes. No mention of this purpose was made at the in-store interface where the email address was recorded, nor was there any reference to Home Depot’s privacy policy which did include very general language that Home Depot argued encompassed the practice.

Furthermore, the OPC found that Home Depot disclosed customer personal information to Meta, not solely as a service provider, but for Meta to use that information both on behalf of Home Depot and for Meta’s own business purposes, including for purposes unrelated to the provision of services to Home Depot.

Under Meta’s terms and conditions for the “Offline Conversions” tool and under its privacy policy, Meta was permitted to use the customer’s information for its own business purposes, including targeted advertising, unrelated to Home Depot. Specifically, Meta could use the information to create “lookalike audiences” to deliver ads across Meta technologies to people with a similar profile to existing offline customers. The OPC found that these uses went beyond Home Depot’s business purposes and even further beyond the reasonable expectations of the customer. Therefore, the OPC concluded that Home Depot must obtain consent for this disclosure.

With respect to consent, the OPC concluded that Home Depot failed to obtain any valid, meaningful customer agreement for its practices of sharing their personal information with Meta. It did not accept Home Depot’s assertion that it had obtained *implied consent* for the practice: it could not rely on its privacy policy and/or that of Meta to obtain consent, and in any event, the explanations provided in those policies were insufficient to support any meaningful consent. Most customers would be completely unaware of the practice, and would not reasonably expect it. Customers’ providing their email address to obtain an e-receipt could not be implied to constitute permission for the information to be used by Home Depot for secondary purposes, or for disclosure to Meta to be used for its own separate business purposes.

Furthermore, it was the OPC’s conclusion that Home Depot could not in any event have relied on implied consent and should have obtained express, opt-in consent because the information was potentially sensitive. While it accepted that in the specific context of Home Depot’s use of Meta’s Offline Conversions tool, the data in question⁴ may not have been sensitive, this conclusion did not preclude the possibility that offline purchases and spending patterns can be sensitive and raise a meaningful risk of harm in other retail contexts. The OPC posited that such personal information could become sensitive in the context where it is shared with Meta to be combined with other information they hold, to create a rich multi-dimensional profile about the individual.

In sum, the OPC concluded that express consent was required for two reasons: that the customer would not have reasonably expected the uses and disclosures that Home Depot would make regarding the personal information, and that the information could become sensitive – both recognized under Canadian privacy law, specifically PIPEDA, as criteria precluding implied consent.⁵

Significantly, the OPC went further and stated that such express consent must be obtained in a transparent and active manner, by opt-in choice, at the time of Home Depot customers’ providing their email, including as to whether to have

⁴ Customer hashed email; date/time of the purchase; transaction ID; sales dollar amount; custom variables for product information and type of transaction, which refer to the general department of the transaction, such as “lumber”, “hardware” or “paint”.

⁵ The OPC stated its reasoning as follows:

While the information in question may not have been sensitive in the circumstances of this case, we find that when requesting an e-receipt in-store, Home Depot customers would not reasonably expect, or have any reason to suspect, that their email address and off-line purchase details would be shared with Meta for the purpose of measuring the impact of Home Depot’s online advertising campaigns. Nor would they reasonably expect that this same information be disclosed to Meta, the world’s largest social media company and one of the world’s largest online advertising platforms, to be used for Meta’s own business purposes including targeted advertising, unrelated to Home Depot.

their personal information shared with Meta, whether for Home Depot's secondary purposes or for Meta's purposes unrelated to those of Home Depot.

Meta Ireland

The [EDPB's Meta Ireland decision](#), released in December, presaged the OPC's determinations in the Home Depot case and arguably undercut the [OPC's 2009 Facebook Findings](#) that collection and use of users' data for advertising purposes was an integral part of Facebook's service, not requiring separate user consent.

The EDPB determined that Meta, through its Facebook and Instagram platforms, could not rely on the GDPR's "contractual necessity" basis for establishing lawful collection and use of users' personal data for behavioural advertising purposes, but needed to obtain consent, separate and distinct from its terms and conditions of use. Its conclusions align with key elements of the OPC's Home Depot decision: not only was separate consent required, but such consent must be actively made – the requirement for opt-in – and transparently sought, on the interface where users initially interact with the platform. Brief reference to such uses in Facebook's Terms and Conditions was inadequate to communicate users' knowledge sufficient to have supported a basis to establish contractual necessity – when the users in all likelihood were unaware that they were agreeing to such uses. To further underscore the lack of contractual necessity as a basis for Meta's data practices, the EDPB made clear that it did not accept Meta's position that use of data for behavioural advertising purposes constituted a core element of its Facebook service. In other words, such use was a secondary purpose requiring separate consent, which could be withdrawn at any time without terminating the user's right to use the Facebook or Instagram service.

The GDPR allows for six legal bases to process data, one of which is consent.⁶ A second basis is "contractual necessity", described as: "processing that is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".⁷

In the words of NOYB - European Center for Digital Rights, Max Schrems' privacy activist non-profit organization that brought the complaint, Meta tried to bypass the consent requirement for tracking and online advertisement by arguing that ads are a part of the "service" that it contractually owes the users.⁸

Meta also argued that a distinguishing feature and commercially essential element of the contract between Meta and its users is that it funds its Facebook and Instagram services with targeted and personalised advertising to the users.

The Irish Data Protection Commission, where the complaint was brought, had agreed with Meta, stating that having regard to what it described as the "clear" terms of the contract, targeted advertising forms a core element of Meta's business model and transaction with users. It concluded that Meta could in principle rely on Article 6(1)(b) of the GDPR

⁶ Article 6(1)(a)

⁷ Article 6(1)(b)

⁸ See: [Breaking: Meta prohibited from use of personal data for advertising](#), NYOB, Jan. 4, 2023.

as a legal basis of the processing of users' data necessary for the provision of its Facebook and Instagram social media services, including through the provision of behavioural advertising insofar as such advertising forms a core part of that service offered to and accepted by users.

The EDPB disagreed, concluding that behavioural advertising is not objectively necessary for Meta to provide its Facebook and Instagram services and is not a core element of it.

The EDPB found that a reasonable user cannot expect that their personal data is being processed for behavioural advertising simply because Meta briefly referred to this processing in the Facebook Terms of Service or because of the "wider circumstances" or "recognised public awareness of behavioural advertising" derived from its "widespread prevalence". Describing the characteristics of behavioural advertising as a set of processing operations of personal data of great technical complexity, which has a particularly massive and intrusive nature and referring to Facebook Terms of Service and Data Policy as including only a very brief and insufficient information that Meta provides about it, the EDPB found it extremely difficult to conclude that an average user can fully grasp it, be aware of its consequences and impact on their rights to privacy and data protection, and reasonably expect it solely based on the Facebook Terms of Service.

The EDPB also referred to the fact that the Facebook Terms of Service do not provide for any contractual obligation binding Meta to offer personalized advertising to users or any contractual remedy if Meta fails to do so. The EDPB pointed to this circumstance to demonstrate that, at least from the perspective of the Facebook user, such data use was not necessary to perform the contract. Providing personalized advertising to its users may be an obligation between Meta and the specific advertisers that pay for its targeted ads in the Facebook service, but it is not stated as an obligation vis-a-vis the Facebook users. Furthermore, the EDPB concluded that Meta's business model of relying on targeted advertising to generate income to support its Facebook service did not make its providing personalized ads necessary to perform the contract.

Conclusions

The OPC's recent Home Depot investigation report and the European Data Protection Board's December decision in the *Meta Ireland* case provide important guidance regarding the evolving transparency rules for online personal data collection and use for secondary purposes, in particular targeted advertising on digital media. Essentially, these two cases point to a requirement to obtain distinct, opt-in and revocable consent for such purposes when they are not within the reasonable expectations of the data subject. While it is arguable that both the Canadian privacy law, PIPEDA, and the GDPR should be interpreted to require such a consent, for reasons particular to the respective jurisdictions, an express requirement for such a proactive exercise of an individual's control over their online information has not been articulated prior to these decisions.

For more information please contact: David Young 416-968-6286 david@dauidyounglaw.ca

Note: The foregoing does not constitute legal advice. © David Young Law 2023