PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

Emily Sharpe
Privacy and Public Policy, EMEA

26 April 2019

Dear Emily,

We thank you for your response (Appendix A, dated 19th April 2019) to our letter (Appendix B, dated 6th March 2019) regarding the searchability of mobile telephone numbers provided for 2FA purposes.

As the response does not directly address our questions, we have attempted to extract the relevant information as answers to our original questions, below. We hope this is an accurate reflection of your positions on this matter.

Your response raises some new questions while a number of others remain outstanding, which we urge you to address.

1) Is it accurate that phone numbers given specifically for security purposes (including 2FA) are now searchable?

> *"[I]n response to feedback [Facebook have] received, [Facebook] have recently revised [their] systems so that new phone numbers added directly through the two-factor authentication flow are not used to match Custom Audiences or deliver ads"*

PI: Your response, although it doesn't say so directly, implies that until "recently" phone numbers added directly through the two-factor authentication flow were indeed searchable.

2) If this is accurate, was this due to a deliberate policy, an oversight, or a bug?

PI: We believe this question was not directly addressed, and urge you to do so.

3) If this is a change of policy, what is your legal basis for repurposing these phone numbers under GDPR Article 6(4)?

> "*Once a user adds their phone number to their Facebook account, and you then decide to use this phone number when setting up the two factor-authentication [sic] feature, it can be used for product and advertising purposes as set out in our Data Policy"*

PI: Your Data Policy (https://www.facebook.com/privacy/explanation) describes information you collect from mobile phones based on their use, not information given for 2FA purposes. Since it is only recently Facebook have set these numbers to non-searchable, what *was* your legal basis for repurposing those numbers given to you for the purposes of 2FA?

4) Are users made aware of the repurposing of the phone numbers given for security purposes?

PI: We believe this question was not directly addressed, and urge you to do so. In the meantime, we can only assume that based on nothing having recently changed other than making these phone numbers non-searchable, that users were not made aware.

5) Can a given user see who has access to this information?

> *"The "who can look me up" setting has been in place for many years. It controls searchability of email/phone numbers as opposed to visibility. [...]*
>
> *"The "Who can look me up" setting applies to all phone numbers you have added to Facebook and defaults to "everyone". Currently the minimum audience you can change it to is friends. This is to enable people who already have your phone number (for example in their contact book) to find you on Facebook*
>
> *"In April 2018, [Facebook] removed the ability to enter another person's phone number or email address into the Facebook search bar to help find someone's profile. Today, the setting called "Who can look me up" controls how people's phone numbers or email addresses can be used to match to their profile in other ways, such as when someone uploads their contact books to Facebook from their mobile phone or when they search for the person in the Messenger app."*

PI: The answer appears to be “no”. Whilst these phone numbers cannot be used for direct searching, they can still be used to add friends based on your mobile contacts - i.e. they are still searched. The best users can hope for is the minimum being set to "friends", and hope that an adversary attempting to find them doesn't have their mobile phone number.

6) Can you confirm reporting by Venkatadri et al that "we found no privacy settings that directly let a user view or control which PII is used for advertising; indeed, we found that Facebook was using the above PII for advertising even if our control account user had set the existing PII-related privacy settings on to their most private configurations. Finally, some of these phone numbers that were usable to target users with did not even appear in Facebook's "Access Your Data" feature"?

PI: We believe this question was not directly addressed, and urge you to do so.

7) What steps, if any, will you take to ensure that phone numbers provided for the purpose of securing accounts are not made searchable?

> *"[I]n response to feedback [Facebook have] received, [Facebook] have recently revised [their] systems so that new phone numbers added directly through the two-factor authentication flow are not used to match Custom Audiences or deliver ads"*
>
> *"Once a user adds their phone number to their Facebook account and then later chooses to use this phone number to enable two-factor authentication, (1) the number can be used used for the purposes set out in the phone number flow and in our Data Policy, including product and advertising purposes and (2) will be searchable to a minimum audience of "friends"— although no longer through the Facebook search bar. However, as noted above, we have recently revised our systems so that new phone numbers added through the two-factor authentication flow are not used to match Custom Audiences or deliver ads."*

PI: We welcome this step of making numbers set purposefully for 2FA non-searchable. We recommend to make clear to the user the distinction between the different flows.

We will publish this exchange in full on our website
www.privacyinternational.org

Your sincerely,

Antonella Napolitano
Policy Officer