PRIVACY INTERNATIONAL

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

Below text as received by email from Emily Sharpe (Privacy and Public Policy, EMEA –Facebook) on 3rd May 2019

(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's follow-up question: 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.

Facebook's response:

We would first like to clarify, as explained in our initial response, that there is currently no way to provide a phone number *specifically* for security purposes as you indicate in your question. Many people choose to enable two-factor authentication using a phone number they have already added to their account.

In addition, we would like to be clear that the “Who can look me up?” settings have been in place for many years and are distinct from the two-factor authentication feature. In April 2018, we *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. But to be clear, people can no longer look someone up via the Facebook search bar. We explain this in our Help Centre here: https://www.facebook.com/help/131297846947406.

Currently 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 friends. This is to enable people *who already have your phone number* (for example in their contact book) to find you on Facebook.

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

PI's follow-up question: We believe this question was not directly addressed, and urge you to do so.

Facebook's response:

We changed this functionality due to the reasons we described in the following blog post: https://newsroom.fb.com/news/2018/04/restricting-data-access/

***"Search and Account Recovery**: Until today, people could enter another person's phone number or email address into Facebook search to help find them. This has been especially useful for finding your friends in languages which take more effort to type out a full name, or where many people have the same name. In Bangladesh, for example, this feature makes up 7% of all searches. However, malicious actors have also abused these features to scrape public profile information by submitting phone numbers or email addresses they already have through search and account recovery. Given the scale and sophistication of the activity we've seen, we believe most people on Facebook could have had their public profile scraped in this way. So we have now disabled this feature. We're also making changes to account recovery to reduce the risk of scraping as well."*

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

Facebook's original response as quoted by PI:

"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's follow-up question: 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?

Facebook's response:

There was no change in policy. We would like to clarify, as explained in our initial response, that there is currently no way to provide a phone number *specifically* for security purposes as you indicate in your question. Many people choose to enable two-factor authentication using a phone number they have already added to their account.

The legal bases pursuant to which Facebook processes phone number(s) added directly by a user to their Facebook profile, as set out in Facebook's Data Policy and 'further information on legal bases' page, accessible from Facebook's Data Policy section entitled “What is our legal basis for processing data?”, are as follows:

- Facebook relies on contractual necessity (Article 6(1)(b) of the GDPR) to process phone number(s) added directly by a user to their Facebook profile for all people who have the legal capacity to enter into an enforceable contract, as necessary to perform Facebook's contract, the Facebook Terms. The processing purposes which are necessary for the provision of Facebook's contractual services, are:
    - To provide, personalise and improve the Facebook Products (with the exception for numbers added by users to their profile directly from the two-factor authentication flow);
    - To promote safety, integrity and security;
    - To transfer, transmit, store or process data outside the EEA, including to within the United States and other countries;
    - To communicate with Facebook's users, for example, on product-related issues; and
    - To provide a consistent and seamless experiences across the Facebook Company Products.
- Facebook relies on its legitimate interests or the legitimate interests of a third party, where not outweighed by the data subject's interests or fundamental rights and freedoms (Article 6(1)(f)) for the processing of phone number(s) added directly by a user to their Facebook profile as follows:
    - For people under the age of majority (under 18, in most EU countries) who have a limited ability to enter into an enforceable contract only, to:
        - Provide, personalise and improve the Facebook Products (with the exception noted under Question 1 for numbers added by users to their profile directly from the 2FAC flow);
        - Promote safety, integrity and security, including through tools focused specifically on threats to people under the age of majority; and
        - Provide non-marketing communications for product or customer service-related issues.
    - For all people, including those under the age of majority, where this processing is actually undertaken:
        - For providing measurement, analytics and other business services where Facebook is processing data as a controller;
        - To research and innovate for social good; or
        - To share information with others including law enforcement and to respond to legal requests.
- Where relevant, Facebook relies on compliance with a legal obligation (Art 6(1)(c) of GDPR) for the processing of phone number(s) added directly by a user to their Facebook profile for processing data when the

law requires it, including, for example, if there is a valid legal request for certain data.

- Where relevant, Facebook relies on protection of a user's vital interests or those of another person (Art 6(1)(d) of GDPR) for the processing of phone number(s) added directly by a user to their Facebook profile for protection of the user's life or physical integrity or that of others, and to combat harmful conduct and promote safety and security, for example, when Facebook is investigating reports of harmful conduct or when someone needs help.
- Facebook may rely on processing for tasks carried out in the public interest (Art 6(1)(e) of GDPR) for the processing of phone number(s) added directly by a user to their Facebook profile for undertaking research for social good and to promote safety, integrity and security, as described in Facebook's Data Policy under "How we do use this information?", where this is necessary in the public interest as laid down by Union law or Member State law to which Facebook is subject.

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

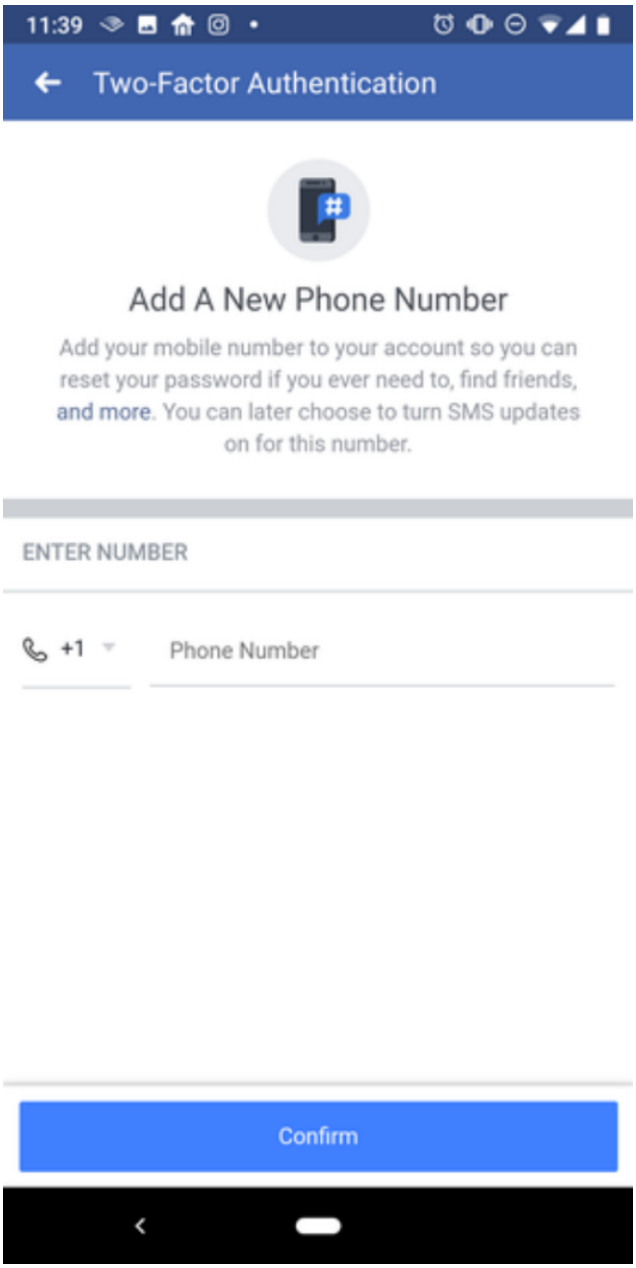
PI's follow-up question: We believe this question was not directly addressed, and urge you to do so. In the meantime, we can only assume that based on nothing having recently changed other than making these phone numbers non-searchable, that users were not made aware.

Facebook's response:

Again, we would like to clarify that there is currently no way to provide a phone number *specifically* for security purposes as you indicate in your question. Many people choose to enable two-factor authentication using a phone number they have already added to their account.

As described in our initial response, 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, the number can be used for the purposes set out in the phone number flow and in our Data Policy, including product and advertising purposes.

We are including a screenshot to illustrate the notice to users:



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

Facebook's original response as quoted by PI:

"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's follow-up question: 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.

Facebook's response:

As explained, the "who can look me up" setting controls the searchability of email/phone numbers. People who want to see what people might be able to access their phone numbers or email, can review the “who can look me up” setting and modify it according to their preferences.

(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's follow-up question: We believe this question was not directly addressed, and urge you to do so.

Facebook's response:

People can manage the information used to show them ads via Ads Preferences. The “Advertisers You've Interacted With” tab lets people know the advertisers who are running ads using a contact list they uploaded that includes your information. We explain that the information may have been collected by the advertiser, typically after you shared your email address with them or another business they've partnered with. You can also hide ads from each of these advertisers via Ads Preferences.

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

Facebook's original response as quoted by PI:

"[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's follow-up question: 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.

Facebook's response:

We would like to reiterate that there is currently no way to provide a phone number *specifically* for security purposes as you indicate in your question. Many people choose to enable two-factor authentication using a phone number they have already added to their account.

We thank you for your feedback on this point. We are currently exploring ways to better communicate the "searchability" aspect of phone numbers, and would welcome the opportunity to discuss this with you at greater length.