GDPR Case Study:
2020-03-11, Google LLC, Sweden

Kinan Dak Albab

Summary In a recent case, the Swedish Data Protection Authority fined Google approximately 8 million dollars for several violations of the GDPR.

This case began in 2017, when the Swedish DPA finalized an audit concerning Google's compliance with articles 5, 6, and 17 of the GDPR, in particular with respect to the lawfulness of Google processing of certain protected personal identifiable information (PII), and compliance with requests from data subjects regarding the removal of their data. This audit produced several orders to Google to ensure future compliance [3].

However, in light of further evidence suggesting that Google did not comply with these orders, a more expanded audit was launched by the DPA in 2018, which concluded on March 11 2020, with an approximately 8 million dollars in fines against Google.

Specifically, the orders issued in 2017 demanded google remove (sometimes called de-index) several web addresses from appearing in results of certain Google searches. The DPA found that Google did not comply with orders to remove two such addresses. Additionally, the DPA took issue with Google's practice of informing web-page maintainers or owners when certain addresses that belong to them where de-indexed.

1 The Violations

The orders issued by the DPA in 2017 requested that Google de-index certain webpages from appearing in search results. In particular, the search results in question relate to searching for a data subject by name.

The right to be forgotten guarantees that a data subject (an individual residing in the EU) have a right to request certain web addressed be removed from the results of searching for personal identifier of that subject (e.g. searching on Google for the subject's name), for reasons such as removing inaccurate or irrelevant information. This right is enchrined in the GDPR, and dates back to cases prior to the implementation of the GDPR [5].

The DPA found that Google did not sufficiently comply with two such orders in 2017. In the first order, the DPA determined that Google adopted "too narrow an interpretation" in terms of which exact web urls were to be de-indexed. My understanding is that Google removed a subset of pages from the search results belonging to a domain that the DPA referred to in the order, and the DPA thought that there were additional pages that needed removing. Additionally, the DPA concluded that google did not de-reference results belonging to the second order in a timely manner without "undue delays" [2,3].

Central to these violations were Google's policy regarding de-indexing of search results. When Google determines that certain web page should not appear in a search result anymore (due to a GDPR request or otherwise), Google informs the owner of that web page of this decision. This notification policy already caused some controversy recently, when Google was asked to de-index news stories discussing Google previous de-indexing of other stories [**?**].

The DPA took issue with this practice due to two reasons:

1. The owner of the webpage can, upon receiving information of a pending de-index, move the content of the page to a different web address or even a different domain, making this new content appear in the search results again, and prompting the data subject to need to go through the cycle of GDPR requests again.

   The content owner may even alter the content (paraphrase it) or its representation (HTML encoding) to make it so that it is difficult to detect automatically that this content ought to be de-index due to its relationship to a previous de-indexing.

The DPA found this to be a grave violation of the intent of the right to be forgetten, that deprives data subjects of that critical right, by turning de-indexing into a cat and mouse chase, and introducing delays between subsequent requests and removes.

2. The DPA deemed the process of informing the web page owner an unlawful processing of protected data. This is in part because Google, as part of the notification, shares some data related to the de-reference origin, which may include some PII of the complaint subject, or may be linked to the identity of that subject via examination of the content of the de-indexed pages.

   For example, if a webpage owner receives notification that a webpage containing information about a sole individual, the webpage would reasonably conclude that the GDPR request may have been issued by that individual.

   The DPA determined that this is a grave violation of the GDPR: it is unlawful second use of data subject's PII to expose it to third parties via the proxy of de-indexing notification [4]. Furthermore, it is detrimental to the right of data subjects to be forgotten, as it exposes that a subject requested action under that right, which may cause subjects to be hesitant to do so in the future, for fear of retribution or reputation damage [2].

Overall, the DPA determined that these violations are part of Google's regular business processes, and are conducted regularly by Google. The DPA assumed that these violations have benefited Google financially, and thus decided to issue a heafty fine against Google, its second largest GPDR related fine to date.

Google's Arugments Google attempted to argue that its notification to the webpage owners, including any attached or inferred PII about the complaining subject, is lawful and protected use, because it falls under legal obligation and legitimate interest. The DPA found these arguments to be invalid [4].

Google announced its intent to appeal this decision [1]. It is unclear to me whether this appeal has taken place (I assume it has), and how far along it has come. The final decision is unclear.

Consequences The fine itself was split into two portions: a smaller portion nearing 2.5 million euros was related to the violation of the two deletion orders from 2017, the larger portion nearing 5 million euros was related to the notification of web page owners.

This demonstrates that DPA's are likely to issue heavier fines for violations that appear to be part of regular business practices of a company. Additionally, it provides additional insights into the limits of "legitimate use", especially when it is counter-balanced by potential indirect harm to established GDPR rights of data subjects.

Additionally, Google in this case acts as a Data controller (in addition to being a processor). Google established that Ireland is a main establishment for part of its operations, but did not explicitly state that search was part of these operations. The Swedish DPA used this to argue that "the one stop" mechanism, which would have otherwise given authority to Ireland's DPA, was inapplicable, and thus arguing that the Swedish DPA is authorized to conduct this inquiry and levy fines.

Personal Opinions In my view, there are certainly viable arguments for why Google may have a "moral" obligation to inform webpage holders that their webpages may be de-indexed. However, there are obvious cases where Google has an obligation to the contrary.

The DPA, in its decision, affirmed that the potential harm such notification may induce on the ability of data subjects to exercise their protected rights under the GDPR outweighs other obligations that Google may have for notifications.

I am not sure I can faithfully agree with such a blanket affirmation. However, I do understand the conundrum. I am curiours whether Google or a company in a similar circumstances may succeed in using a legitimate interest (or even a public interest) argument for such notification, if the exact specifics of which webpages were being de-indexed and what was the reasoning behind the compaints for having them de-indexed. I would assume that cases where politicians or public figures requesting that certain articles with substantive revelations of bad conduct be removed from search result would be treated differently in the interest of the public, to name one example.

This case is interesting for researchers and systems designers, in particular because it highlights how processes that may not be part of the core system or its privacy component (in this case the search engine) may still cause privacy issues, either directly via revealing PII, or indirectly via linkage.

Furthermore, the desicion to make notification of de-indexing a part of the process of delisting search results prob-

ably was not taken by systems designers or for technical considerations. It is reasonable to assume that it included many stakeholders including product designers, high-level administrators, and legal and PR professionals, far more than it included technical privacy researchers or systems designers. This shows a need for greater inclusion of privacy professionals in various aspects of product development, including less-technical decision making.

References

[1] Google to appeal swedish data watchdog 7m fine. https://www.politico.com/news/2020/03/11/google-to-appeal-swedish-data-watchdog-7m-fine-125460. Accessed: 25-09-2020.

[2] Sweden fines google $8 million for right-to-be-forgotten violations and demands it keep websites in the dark. https://venturebeat.com/2020/03/11/sweden-fines-google-8-million-for-right-to-be-forgotten-violations-and-demands-it-keep-websites-in-the-dark/. Accessed: 25-09-2020.

[3] The swedish data protection authority imposes administrative fine on google. https://edpb.europa.eu/news/national-news/2020/swedish-data-protection-authority-imposes-administrative-fine-google_en. Accessed: 25-09-2020.

[4] Swedish dpa fines google in rtbf case. https://iapp.org/news/a/swedish-dpa-fines-google-in-rtbf-case/. Accessed: 25-09-2020.

[5] What is the 'right to be forgotten'? https://www.bbc.com/news/technology-27394751. Accessed: 25-09-2020.