Forget Me Not: 'Right to Be Forgotten' Limited to the EU

October 3, 2019

The "right to be forgotten" does not require internet search engines in the European Union to purge search results displayed outside the European Union. So held the Court of Justice of the European Union ("CJEU") last week, construing the European Union's General Data Protection Regulation ("GDPR") in a way that promises substantial relief to Google and its fellow search engines. The CJEU had little relief to offer, though, to other businesses: Most will still have to honor right to be forgotten requests even where the data resides outside the European Union.

The Right to Be Forgotten. When GDPR took effect last year, it gave EU individuals (and those outside the European Union whose data is processed in connection with a business's EU establishment) the right to ask an organization holding their personal data (a "data controller") to erase it. For example, a right to be forgotten request typically must be honored if the data is no longer necessary for the purpose it was originally collected, or if the data was processed based on consent, but the individual withdraws that consent.

But the right is not absolute. Under the GDPR, the requester's interests must be balanced against other fundamental rights and freedoms, such as freedom of expression or the right of defense. In some circumstances, then, the data controller can reject the request or respond by purging only some of the requester's data.

The right in the GDPR expands a judge-made rule. In a 2014 case involving Google Spain, the CJEU held that internet search engines could be required to "de-reference" links to third-party webpages. That is, if Mr. Gonzalez from Spain was concerned about his personal data surfacing on third-party webpages via Google searches, then Google Spain could be ordered to stop displaying those pages in search results. The GDPR expanded that right (1) to allow individuals to make such requests to all data controllers, not just search engines, and (2) to require that data be deleted where it lives, not just omitted from search results.

Left open—until now—was the question of whether a controller responding to a "right to be forgotten" request had to look beyond EU borders and include non-EU-based data in its response.

For Search Engines, the Right to Be Forgotten Now Stops at the EU's Edge. Picture Jeanne sitting at her computer in Paris, running a Google search. She starts at google.com, the main site of Google's U.S. parent company. But Google geo-locates Jeanne's IP address to France and automatically takes her to google.fr. Likewise, Frans in Amsterdam is referred to google.nl, Maria in Frankfurt to google.de and so on. Now Jeanne asks Google to "forget" her. Can Google limit the search, and purge, of its records to google.fr? Or must its efforts reach its other national sites in the European Union (.de, .nl, .es etc.), or even beyond the Union (.ca, .jp, .au etc.)?

Those were open questions prior to the new CJEU ruling. The French data protection regulator ("CNIL") had required Google to implement accepted right to be forgotten requests not only on its EU domains but also on its non-EU sites. Google refused and challenged the order before the Conseil d'Etat—France's highest administrative court—which referred the matter to the CJEU.

The CJEU held, in a nutshell, that a search engine's response to a right to be forgotten request should be confined to the European Union. The Court noted that ordering erasure on a global basis would best meet the GDPR's objectives but nevertheless found that the GDPR *currently* imposes no obligation on search engines to implement a request to be forgotten outside the European Union.

The Court added that even if such a global right existed, it could not be enforced, as there are currently no cooperation instruments between EU and non-EU authorities. In contrast, the Court found that because there are existing EU-wide cooperation mechanisms, a valid request to be forgotten should be implemented in all EU member states and not only in the member state where the requesting individual resides.

Importantly, the CJEU also required search engine operators to take "sufficiently effective measures" to prevent EU-based individuals accessing "forgotten" links by navigating to non-EU google domains. Put another way, once Jeanne has been "forgotten" by google.fr and other EU google domains, Frans in Amsterdam should not be able to use google.com to find the "forgotten" records about Jeanne. The Court did not specify what technical measures should be taken to implement this but asked local authorities to assess the sufficiency of geo-blocking.

The Court also clarified that EU member state regulators or courts could still order that a request to be forgotten be implemented outside the EU on the basis of national

standards for the protection of fundamental rights. The door thus remains ajar for EU member states to impose the right to be forgotten outside the Union on Google et al.

What About Non-Search Companies? Non-search companies will likely still be required to honor GDPR right to be forgotten requests, irrespective of whether the data is held inside or outside the European Union. This is because the question referred to the CJEU was specific to the search engine context on the internet. The fundamental rights arguments the Court used to justify its conclusions, including the freedom of internet users to information, are unlikely to apply in most circumstances.

That said, the territorial limitation of the right to be forgotten may apply in industries analogous to search engines and where data is made publicly available on the internet, such as on social media platforms or through data-brokering databases. In these contexts, many of the same arguments that the Court relied on to reach its conclusion would equally apply.

The Balancing of the Right to Be Forgotten with Sensitive Data. In a separate decision issued on the same day, the CJEU clarified how the right to be forgotten is to be balanced with other competing rights when sensitive personal data is concerned. Under EU law the processing of "special categories of personal data"[1]—often referred to as sensitive data—is prohibited, unless exceptions apply, including valid consent or where justified by substantial public interest. Similarly, the processing of personal data relating to criminal convictions and offences is restricted and requires appropriate data protection safeguards.

The second decision also arose from a referral from the Conseil d'Etat regarding a request to be forgotten made to Google: Here the operator refused to de-reference various links that appeared in search results for the names of EU residents. The links led to third-party websites that contained sensitive personal information relating to individuals' political opinions, religious or philosophical beliefs, sex life and criminal convictions.

The CJEU previously established that just showing a link in a list of search results can significantly affect the fundamental rights to privacy and data protection because it enables a profile of the data subject to be formed. Under the GDPR, the operator of the search engine needs to strike a balance between the rights of the person making the request to be forgotten and those of users potentially interested in that information.

---

[1] "Special categories" include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The Court's decision now requires that this test is made on the assumption that generally the data subject's rights prevail over other users' right to freedom of information.

Consequently, a search engine receiving a request to be forgotten relating to a link to a website on which sensitive data is published must ascertain whether the inclusion of that link in the search results is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing the information. This assessment has to be made based on all relevant factors of the particular case, including the seriousness of the interference with the data subject's fundamental rights to privacy and protection of personal data.

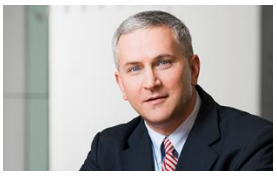
The search engine has to conduct a similar balancing exercise in the case of links leading to information on legal proceedings and information relating to criminal convictions. If the balance tips in favor of the freedom of information of potentially interested internet users, the Court requires the search engine to adjust the list of results in such a way that the overall picture reflects the current legal position. For example, a link referring to a site reporting an acquittal of the searched person should be displayed ahead of reports about the initial allegations.

Again, the decision is unlikely to have a significant impact beyond the search engine space, with the exception of other online content providers, such as news aggregators or similar service providers. Nevertheless, all businesses can be guided by the decision when assessing competing fundamental rights when they do arise.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK



Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

WASHINGTON, D.C.

Jeffrey P. Cunard
jpcunard@debevoise.com

Luke Dembosky
ldembosky@debevoise.com

LONDON

Jane Shvets
jshvets@debevoise.com

Christopher Garrett
cgarrett@debevoise.com

Robert Maddox
rmaddox@debevoise.com

PARIS

Alexandre Bisch
abisch@debevoise.com

FRANKFURT

Dr. Thomas Schürrle
tschuerrle@debevoise.com

Dr. Friedrich Popp
fpopp@debevoise.com

Jennifer Deschins
jdeschins@debevoise.com