Google Belgium vs The Belgian DPA: A GDPR Case Study

Jonathan Weisskoff
Brown University

Abstract

On July 7, 2020, the Belgian Data Protection Agency (DPA) imposed a fine of 600,000 EUR (681,400 USD [11]) on Google Belgium for violation of the European General Data Protection Regulation's (GDPR's) "Right to Erasure." The complainant, a Belgian resident and CEO of a large company who had a history of involvement in political parties, requested that Google remove search results that reported that he had been accused over 10 years ago of harassment. He also requested the removal of search results that implied his affiliation with a political party which he had since repudiated. The Belgian DPA ruled in favor of the complainant regarding the former request, on the grounds that the accusations were old and had long been dismissed as unfounded, so were no longer relevant to the public. The DPA ruled against the complainant regarding the latter request, on the grounds that the search results did not imply the complainant's support of said political party. The DPA required Google to delist the forbidden results from searches in the EU Economic Zone but did not require Google to dereference the results globally. The verdict is significant in that it 1. imposes the largest fine yet by the Belgian DPA, 2. clarifies the line between protecting the individual and making data available for the public welfare. 3. deems Google's Belgian subsidiary as an extension of its parent company Google LLC, 4. limits the applicability of the "one stop shop" rule to violations where the data controller/processor's main EU establishment is itself the data controller/processor, 5. requires the removal of search results beyond the jurisdiction of the Belgian DPA but not from the whole world. I argue that it is questionable whether Google could have been expected to predicted this verdict so as to avoid the fine, and that that the verdict's position on the "one stop shop" rule may undermine the intent of the rule.

This article was written 9/27/2020 for a Brown University Computer Science course: *Privacy Conscious Computer Systems*, taught by Prof. Malte Schwartzkopf, PhD.

1 Background

The case of *Google Belgium vs. Belgian DPA* deals with the legal boundaries of the "Right to Erasure", the jurisdiction of an EU member state's DPA, including the applicability of the "one stop shop" rule for cross-border violations, and territorial extent of GDPR enforcement. These can be better understood in the context of their legal definitions and/or histories.

Right to Erasure The "Right to Erasure," also referred to as the "Right to be Forgotten," was first enshrined in EU law in the European Data Protection Directive of 1995 and further developed through the UK DPA's ruling in 1998. Among other rights, it gave individuals the right to prevent the processing of data when doing so "caus[es] or [is] likely to cause substantial damage or substantial distress" where such damage or distress is "unwarranted". An exception to this rule was allowed, among other exceptions, where the information was published in the public interest of freedom of expression [10].

In 2014, the E.U. Court of Justice (CJEU) ruled in *Google Spain v AEPD and Mario Costeja Gonzalez (i.e. the Spanish DPA)* that the "right to erasure" applied to "outdated and irrelevant search engine results unless there was a public interest in the data remaining available." It therefore required that Google remove such search results [10].

The European Data Protection Directive's "right to erasure" was incorporated into the GDPR's Article 17, stating:

> 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies... (c) the data subject objects to the processing. ... 3. [with the exception of when] the processing is necessary... (a) for exercising the right of freedom of expression and information. [7]

Jurisdiction of an EU Member State's DPA The GDPR,

Article 3, legislates that for a DPA of an EU member state to have the authority to prosecute a data controller or processor, one of two conditions must be met: either the controller or processor has an establishment in the said member state (Article 3.1), or the data subject is a person inside the territory of the said member state (Article 3.2). The former of these conditions had already been established by prior legislation. In the latter condition, if the controller/processor has a "main establishment" in another EU member state, then the "one stop shop" rule stipulates that only the DPA of that other state has the authority to coordinate a prosecution (Article 56.1). This rule is intended to enhance efficiency and prevent companies from being subjected to the threat of prosecution by multiple DPAs [4, 9].

The aforementioned ruling of the CJEU in the case of *Google Spain* established that the Spanish DPA has juridical authority to prosecute Google by virtue of the fact that Google Spain, a subsidiary of Google LLC, is in Spain (as per condition 1, above), even though Google LLC, the data controller and processor, is in California. The rationale given for this ruling is that Google Spain is effectively an extension of Google LLC, and thus can be charged as if it were Google LLC. It should be noted that the *Google Spain* case did not touch upon the "one-stop shop" rule since it was litigated before the GDPR was legislated [6].

Territorial extent of GDPR enforcement In 2016, before the GDPR was adopted, CNIL, the French DPA, fined Google 100,000 EUR for violating the right to erasure by not delisting search results, and demanded that Google delist offending search results globally, since a localized delisting would not effectively protect the data subject. Google appealed to the CJEU, arguing that that if the EU demanded that search engines remove results from third party countries, then third party authoritarian regimes might seek to curtail freedom of expression by demanding removal of search results from the EU. In 2019, the CJEU released its ruling which largely sided with Google stating that the results only had to be delisted from the EU and not globally. The rationale for this ruling was that the EU legislature hadn't "chosen to confer a scope which goes beyond the territory of the EU Member States" [8] and third party states may have differing attitudes towards balancing the right to erasure and the right to freedom of expression. The CJEU did, however, require Google to implement measures that would "effectively prevent" or "seriously discourage" users in the EU from accessing delisted links through non-EU domains, for example, by geo-blocking [12].

2 Case and Verdict

The complaint On August 12, 2019, a Belgian resident who held the position of CEO of a large company and who had a history of participation in political parties, filed a complaint with the Belgian DPA that Google had refused his[1] request to delist search results that he considered harmful to his reputation. He listed 12 results, covering two categories of harm: 1. results that mentioned his being accused of harassment over 10 years ago, and particularly those results that did not mention that the accusation had been dismissed by the courts in 2010 due to lack of evidence, 2. results that suggested that he was affiliated with a political party which he has since repudiated [9].The latter of these is of particularly sensitive nature according to the GDPR's Article 9 that lists data about a person's "political opinions" among the "special categories" that require a higher level of protection [7].

The verdict On August 14, 2019, the Belgian DPA accepted the complaints and set up a hearing for May 2020. On June 14, 2020, the DPA publicized its verdict. Of the 12 URLs that the complainant had requested be delisted, the DPA ruled in favor of the complainant regarding those URLs which showed the complainant to have been accused of harassment. It explained that these URLS violated the complainant's right to erasure, and that an exception, due to freedom of expression (GDPR Article 17.3(a)) does not apply since the truth of the accusations had never been established and the accusations were over 10 years old making them "irrelevant" [9]. Google, the DPA stated in a press release, was "particularly negligent" in refusing the complainants' requests for delisting, as it "had evidence of irrelevance and out-of-date facts" [1]. Thus, the DPA found Google in violation of both Article 17 (the right to erasure) and Article 6 (lawfulness of processing) since its continued processing of the complainant's data was unlawful. As a penalty for these two violations, the DPA imposed a fine on Google of 500,000 EUR [2, 6].

Furthermore, the DPA found Google's response to the complainant's requests for delisting to be lacking in transparency, and hence to be in violation of Article 12 of the GDPR which requires a data controller to explain in "a concise, transparent, intelligible and easily accessible form, using clear and plain language" why it refuses a request from a data subject to exercise their rights under the GDPR. Google had merely written the complainant that "[a]fter examination of the balance between interests and rights associated with the content in question, including factors such as that your role in public life, Google has decided not to block it," which the DPA said left the complainant "confronted with an incomplete ground for refusing his request that did not allow him to know or understand completely what motivated Google." As a penalty for violating this article, the DPA fined Google an additional 100,000 EUR [2, 6].

The DPA ruled against the complainant regarding the URLs which allegedly implied an affiliation between the complainant and a political party, because it did not find these links

[1] Although the gender of the complainant is not officially documented, for expressive convenience, I reference him by male pronouns, as does the verdict.

to imply the complainant's support of said party, but only to show that the complainant had professional ties with the party and that the party supported the complainant, and Article 9 only protects data about a subject's political opinions [2].

As a result of this verdict, the DPA required Google to delist the offending results from the EU Economic Zone, since delisting from just Belgium would not prove "useful" in protecting the complainant (presumably due to ease of travelling between the borders of EU member states to access the listing from a different state). In this decision, it followed the precedent handed down by CJEU to Google vs CNIL (2016), mentioned in Section 1 [9].

Google replied that it would challenge judgement in the courts [5].

Judicial authority The DPA ruled that it is vested with the authority to prosecute Google since Google Belgium is within its member state, as per the precedent set by the ruling in *Google Spain* [6] mentioned in Section 1. Google replied that since its main EU establishment is in Ireland, the "one stop shop" rule applies, giving only the Irish DPA authority to initiate proceedings against it. The Belgian DPA dismissed this argument, explaining that since, by Google's own admission, its Irish establishment was not in charge of listing search results, its Irish establishment is therefore not the data controller/processor, (rather, the controller was, by Google's admission, Google LLC, headquartered in California,) so the one stop shop rule does not apply [2].

3 Legal Significance

The verdict of Belgian DPA vs Google Belgium has legal significance in several ways:

1. The case involved the largest fine levied by the Belgian DPA by an order of magnitude (the next largest fine is 50,000 EUR). This demonstrates the Belgian DPA's commitment to prosecuting violations of the GDPA with more forcefulness than it had in the past.

2. If the verdict is upheld in the courts, then it sets a precedent for determining what is a valid exception to the right of erasure: If an accusation is old and unfounded, then it is not protected under the right of freedom of expression, even if the data subject is a public persona.

3. The verdict builds upon the precedent of *Google Spain* to treat subsidiaries of Google as extensions of Google LLC so that they can be prosecuted as data controllers. It thus enshrines this precedent more strongly into EU law.

4. The verdict denies the applicability of the "one stop shop" rule since the data violation under question is not controlled by the defendant's main EU establishment. A similar judgement was reached in *Google vs. CNIL (2019)*, where CNIL famously fined Google 50 million EUR for violations of the GDPR on Google's Android platform [3]. The Beligan DPA's verdict adds to this precedent. Incidentally, Google wrote to the Irish DPA toward the end of our case's litigation period saying that they would no longer argue that the one-stop shop rule applies to activities that are under the control of Google LLC, indicating that they accept this verdict [6].

5. The verdict is also interesting in that it follows the the ruling of the CJEU in *Google vs CNIL (2016)* that limits the scope of the requirement for delisting to the EU member states. By not challenging the boundaries of this ruling, it further enshrines it into EU law.

4 Discussion

Was Google negligent? Google's key mistake in this case was that it assumed that since the complainant was engaged in public political life, (as it had evidence that the complainant was "a member of a political cabinet of a minister of the Y Party twenty years ago," "participated as a speaker" in the Y Party congress a few years ago, "gave a talk to the Y Party" a few years ago, and "worked in the study center of the Y Party"), old information about his having been accused of harassment was protected under the right of freedom of expression. The Belgian DPA's verdict clarified that the right to freedom of expression does not protect the information, since it is unfounded and old and therefore is considered to be no longer relevant, and that this is so even for a political figure. It is unclear whether it is fair to fine Google for negligence in not drawing this same conclusion, since what is considered to be "old" "unfounded" and "irrelevant" information about a political figure may vary from case to case, and from culture to culture, and is thus debatable.

Is the one-stop shop rule being undermined? The Belgian DPA determined that the one stop shop rule doesn't apply in our case, since Google's main establishment in Ireland does not control the decisions regarding the privacy violations under question. In this decision, it concurred with CNIL in *Google vs CNIL (2019)*, as mentioned in Section 3. However, this approach seems to undermine the aim of the one-stop shop rule, which, as stated in Section 1, seeks to channel all litigation against a company through just one DPA so as to streamline the litigation process and to remove the threat against a company of litigation from multiple DPAs. Given this rationale, it does not seem reasonable to limit the one-stop-shop rule to only those cases where the company's main EU establishment is also the controller of the violation under examination.

5 Conclusion

The Belgian DPA prosecuted Google Belgium for violating a Belgian resident's "right to erasure" and demanded that it delist the offending results from EU territories. In so doing, the DPA clarified the limitations of freedom of expression about a public persona. Due to the cultural and circumstantial subjectivity of the matter, however, it seems questionable whether Google was guilty of negligence in interpreting the right to freedom of expression more liberally. In holding Google Belgium responsible for Google LLC, the verdict builds upon the precedent set in *Google Spain* of treating a subsidiary of a foreign company as an extension of that company. In denying the applicability of the "one stop shop" rule, the verdict exposes online companies like Google to litigation from multiple member state DPAs, a consequence that may run contrary to the intent of the rule. In not requiring a worldwide delisting of the offending URLs, the verdict follows the ruling of the CJEU in *Google vs. CNIL (2016)*. The long term consequences of this case remain to be seen and will depend upon the final ruling handed down by the EU appeals court.

References

[1] Google faces €600,000 privacy fine in Belgium, 2020. brusselstimes.com.

[2] Peter Craddock and Vincent Wellens. What does the new Google decision by the Belgian DPA mean for other organisations?, 2020. lexology.com.

[3] Denise Lebeau-Marianna. Eu: How CNIL fined Google - insights on the One Stop Shop mechanism, 2019. dataguidance.com.

[4] Lokke Moerel. What happened to the one-stop shop?, 2019. iapp.org.

[5] Aaron Nicodemus. Google fined $670k for violating GDPR's 'right to be forgotten', 2020. compliance-week.com.

[6] Litigation Chamber of the Belgian Data Protection Agency. Decision on the merits 37/2020 of July 14, 2020, 2020.

[7] The European Parliament and the Council of the European Union. Regulation (EU) 2016/679 of the European Parliment and of the council. *Official Journal of the European Union*, 2016. eur-lex.europa.eu.

[8] Mary Samonte. Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law, 2019. europeanlawblog.eu.

[9] Gilles Waem, Heidi; Hachez and Camille Vermosen. Belgian DPA imposes a €600,000 fine, its highest fine ever, on Google Belgium for non-compliance with right to be forgotten, 2020. lexology.com.

[10] Taylor Wessing. The evolution of the EU's 'right to be forgotten', 2019. lexology.com.

[11] Aoife White. Google Gets Record Belgian Privacy Fine Over 'Right to Be Forgotten', 2019. bloomberg.com.

[12] Serena Wong. Google v. CNIL: EU Rules that Right to be Forgotten Does Not Apply Globally, 2019. jolt.law.harvard.edu.