Client Update

A New Ruling by the French Data Protection Authority: Is the Right to Be Forgotten Crossing the Atlantic to the U.S.?

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

PARIS
Frederick T. Davis
ftdavis@debevoise.com

FRANKFURT
Dr. Thomas Schürrle
tschuerrle@debevoise.com

Eve Leclercq
ealecler@debevoise.com

France's data protection authority, the *Commission Nationale de l'Informatique et des Libertés* ("CNIL"), has ordered Google to delist several third-party links from search results across all of Google's worldwide search websites—not only from its domains directed towards Europe, such as "google.fr," but also the main U.S. site at google.com, among others. This order follows a 2014 European Court of Justice ("ECJ") ruling that individuals have a "right to be forgotten." The proposed EU Data Protection Regulation will likely further strengthen and extend this right.

WHAT IS THE "RIGHT TO BE FORGOTTEN" IN THE EU CURRENTLY AND TO WHAT EXTENT CAN NATIONAL AUTHORITIES SANCTION NON-EUROPEAN COMPANIES?

The 2014 Google case[1] involved a subsidiary from Google located in Spain, and jurisdiction of the Spanish courts over Google's U.S. parent was anything but certain. In its ruling, the ECJ clearly stated that EU data protection rules are applicable regardless of the location of the company processing the data, so long as the company has a subsidiary or a branch in Europe. In the view of the ECJ, EU data protection rules are not only applicable to the search engine's EU subsidiaries, but also to its sites located outside the EU. Such an extended territorial reach of EU rules has been, and remains as of today, contested by Google, leading effectively to the CNIL's decision. The ECJ decision also

[1] Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=361347.

confirmed that EU data protection rules were applicable to search engines, which were determined to fall within the definition of "controllers."[2]

The decision also held that, because individuals had the right to control search results directing readers to news stories or information about their lives under applicable data protection rules, they could request that these links be "delisted" from a search engine's results. The ruling does not affect the underlying news stories or other personal information, which remain accessible on the website that originally published them, and their removal from the original website would require separate proceedings. In addition, the ECJ held that the right to be forgotten is not absolute and must be balanced against the fundamental rights of others to freedom of expression. Indeed, the links in these search results may be delisted only to the extent that the underlying news story or website to which the search result refers is no longer relevant to the original purpose for which the personal information was collected and published.

So far, the ECJ decision has effectively left it to search engine operators to provide a procedure for delisting links in search results upon request from individuals, over which data protection authorities of the member states retain some control. Currently, an individual seeking delisting of a link to their personal information may fill out a form made available on all major search engines.[3] However, no official criteria were published indicating when the provider would have to accept the delisting request. Unfortunately, the ECJ did not provide much guidance in its decision. Seeking to fill in this gap, the Article 29 Working Party[4] suggested that, in a case involving a request to remove such a link from the search engine's results, a court should consider: (i) the situation of the individual; (ii) the quality of the search data; and (iii) the place and method of the underlying publication.

In response to the ruling, Google has established an online form where individuals may request the delisting of search results from Google's applicable

---

2 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data on the free movement of such data, Article 2(d).

3 Google regularly publishes statistics on the number of delisting requests received and their sources, but does not provide any number regarding the actual number of requests accepted.

4 The Article 29 Working Party is a working group set up under Article 29 of the 1995 Directive on Data Protection to examine questions arising from the application of the directive and to propose relevant changes in its provisions to the European Commission.

European domains that link to a news story or website containing the individual's personal information.[5] Google has reportedly received over 250,000 requests to remove such links since the ECJ's 2014 ruling.[6] Commentators have noted that Google has only delisted around 40% of these requests and has not offered transparency in its criteria for making these decisions.[7]

U.S. courts, by contrast, are expected to be reluctant to follow suit. U.S. courts so far have been wary of placing an individual's privacy rights above the First Amendment's protections for historical reporting and dissemination of factual information. While there is no decision in place dealing with the delisting of links to information like in the ECJ case, the decision in the *Hearst* case is a reasonable indicator where U.S. courts are coming from: The U.S. Court of Appeals for the Second Circuit held that a newspaper was not required to remove stories about a woman's arrest, even though the arrest was later expunged from her record.[8] In so holding, the judge observed that the expunged record is a legal fiction that "does not and cannot undo historical facts or convert once-true facts into falsehoods."[9] Although in a recent defamation case before a New York state trial court, a judge commented that a statutory "right to be forgotten" would, "under certain conditions, [] give[] plaintiffs the opportunity to attain the redress they deserve,"[10] the comment remains an outlier without precedential effect.

---

5 The form is available at https://support.google.com/legal/contact/lr_eudpa?product=websearch.

6 *See Europe's Expanding 'Right to Be Forgotten'*, NEW YORK TIMES (Feb. 4, 2015), *available at* http://www.nytimes.com/2015/02/04/opinion/europes-expanding-right-to-be-forgotten.html.

7 For example, a number of academics have signed a letter to Google asking for further transparency around its treatment of these requests. *See Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data*, *available at* https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd.

8 *Martin v. Hearst Corp.*, 777 F.3d 546, 552 (2d Cir. 2015).

9 *Id.* at 551.

10 *Anonymous v. Does*, 151769/2013 (NY Sup. December 3, 2014) *4.

HOW DID THE GOOGLE CASE SET THE STAGE FOR EXTRA-TERRITORIAL ENFORCEMENT OF EU DATA PROTECTION LAWS IN THE UNITED STATES AND ELSEWHERE?

On May 21, 2015, the CNIL[11] decided to open a formal proceeding[12] against Google concerning the company's non-compliance with French data protection law. Google had displayed search results, as well as EU subsidiary-arranged advertising links, that related to the searched terms that had been the subject of delisting requests. The CNIL determined that Google fell under the authority of EU data protection regulators.

Following numerous complaints from people who had applied without success to delist the links referring to websites with their personal information from Google's search engine, the CNIL had asked Google to delist these links for 21 such individuals. Google ultimately complied with nine of these requests, but limited the removal to the search results appearing on its French domain "google.fr."

The CNIL then ordered Google to delist these results from all of the company's search engine's domains, including its non-EU domains such as "google.com." Although Google did so for its other European domains, it continued to refuse to delist the search results at issue for its domains outside the EU, which—according to Google—are not widely used within Europe.[13] Consequently, the CNIL decided to pursue the company for non-compliance with French data protection rules.

If Google does not comply with the request from the French authority, the CNIL will be in a position to levy sanctions of up to € 300,000 against the company for violation of the French data protection law.[14]

---

11 *See* Commission Nationale de l'Informatique et des Libertés decision No. 2015-047, May 21, 2015.

12 The CNIL decision is in particular based on: (i) the French Law No 78-71 [1978], *loi relative à l'informatique, aux fichiers et aux libertés*; and (ii) the ECJ decision C131/12 [2014], *Google Spain SL v. Agencia Española de Protección de Datos*.

13 *See* Google's answer to the CNIL, letter dated April 24, 2015.

14 *Loi No 78-71 relative à l'informatique et aux libertés*, Article 47.

IS THE GOOGLE CASE JUST AN ISOLATED COURT DECISION, OR DOES THIS HERALD LARGER CHANGES IN EU PRIVACY AND DATA PROTECTION LAWS?

The Google case is illustrative of current trends in European data protection litigation and enforcement: for example, a lawsuit was recently brought in Belgium accusing Facebook of breaching European data privacy laws, and Germany has ordered Google to change the way it collects and combines its user data. Similar cases are to be expected in the near future, especially now that the EU is currently reforming its legislation concerning the protection and privacy of personal data.

On June 15, 2015, Ministers of the Council of the European Union determined a general approach to the reform proposal relating to the Draft on Data Protection Regulation.[15] Negotiations between the European Parliament and Council will start on June 24, 2015, with the aim to reach an agreement before the end of the year.

The proposed Data Protection Regulation[16] would likely strengthen and extend the right to be forgotten and could impose sweeping changes to the EU data protection landscape, affecting EU and global companies alike:

- *Harmonization and expansion of regulations*. The proposal introduces a single set of rules on data protection across the EU, also applicable to non-European companies, when they offer goods or services to EU residents or when monitoring their behavior (Article 3.2). A fine of up to 2% of annual worldwide turnover could be imposed on companies that do not comply with these rules (Article 79).
- *Increased accountability for data secur*ity. The proposal would also heighten responsibility and accountability for the processing of personal data. For example, companies and organizations will be obligated to notify the national supervisory authority immediately of a serious breach of personal data (Article 31).
- *Role of national data protection authorities*. The proposal also introduces the possibility for EU organizations to deal exclusively with the national data

[15] The Regulation will be accompanied by an EU Directive applying to general data protection principles and rules for police and judicial cooperation in criminal matters, for both domestic and cross-border transfer of data.

[16] Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on free movement of such data, COM(2012) 11 final, 2012/011 (COD) [2012].

protection authority of the member state in which they have their principal place of business (Article 48). Individuals could similarly refer complaints to the data protection authority in their country, even if their data is processed by a company located outside the EU.

- *Limitations on data privacy*. Some limitations on individuals' data privacy are nonetheless included in the proposal, including, for example, exceptions to protect public security or the rights or freedoms of others (Article 48).

The EU's latest proposal represents a new legal framework for the unified protection of personal data in member states. National legislatures across Europe are also moving towards stricter regulation of personal data protection.[17] As technology continues to develop and the need for new methods of personal data protection increases, additional regulations are likely to follow.

* * *

Please do not hesitate to contact us with any questions.

[17] For example, in Germany, a draft law (*Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts*) was adopted on February 4, 2015 to improve consumer protection by enabling particular protection organizations and trade associations to file injunctions against companies violating data protection provisions for consumers.