



Data Privacy Detective Podcast – Episode 2 – Google and European Data Privacy

Oct 09, 2016

Categories:

[Blogs](#)

[Podcast](#)

[Publications](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

The Court ruled that as the guardian of the fundamental human right to privacy under European Union principles, Google was declared to be the controller of every link on its search engine. And as controller, this meant that Google was directly responsible for making sure that every link involving European citizens conformed to EU data privacy rules. The ECJ forces Google to delist a site that was determined to invade a European citizen's privacy rights. While sometimes cited as a decision that people have a right to be forgotten, the decision was more narrow and pointed than that – and it had a dramatic effect on Google.

Google respected the decision of the highest court in Europe, and that meant giving Peter Fleischer a monumental job. Google set up a system for European residents to object to listings of websites that contained material to which they objected. Google – as controller in the eyes of the ECJ – thus took on the task of making individual decisions about whether to link or de-link to sites to which European citizens objected. More specifically, the decision balanced the public interest in accessing public information and expression against individual privacy rights, in this case having to do with how long information about an individual could be posted by a third party over the individual's objection, six months being the general EU rule for when information is no longer appropriate on balance for continuing disclosure. The action step ordered by the Court was for Google to delete the individual URL linked to the successful claimant in the ECJ.

Peter first responded by deleting the URL on the European suffixed Google sites, but not on www.google.com. But the EU said that was not enough – that Google should delink from Google.com as well, which is a US-based site. Google agreed. Peter then hired a large workforce to implement the effect of the decision. For about a year after the decision, Google personnel have supervised 1 ½ million

individual decisions whether to accept or reject individual requests, based on European data privacy standards. Peter reported that about 40% of Google's decisions have been to delink and 60% of the time not to delink.

He shared from the heart deep concerns about what the ECJ's decision could mean on a broader basis. Here the EU was applying its standards worldwide in effect by forcing a delinking on google.com. While that may seem benign in the case of the one individual, there is no international court of privacy, nor is there an international agreement on data privacy standards. What, Peter asked, if Pakistan's highest court orders Google to delete any site that defames Islam? What if Turkey orders Google not to link to any site containing material that opposes actions of the Turkish Government? What if Thailand orders Google to delink with any site containing language that demeans the King or his immediate family, a crime in Thailand? Or if Russia orders Google to delink with any URL that claims that being gay is consistent with human dignity, under current Russian rulings? What would this do to the free expression of thought, and how could the internet be global under such impossible demands of governments with different standards on what is private and what is not?

Or consider that the highest court in Colombia and the influential Second Circuit Court of Appeals in the United States have both ruled that there is no right to be forgotten under Colombian or U.S. law. In that case, will Google be subjected to demands from Colombian or U.S. authors if it delinks to a URL because the ECJ says it must, whereas a Colombian or U.S. Court may instruct Google not to delink out of an interest to free speech and comment?

This is only one glimpse into the evolving global battle over data privacy that faces technology providers seeking to expand the worldwide web. In the absence of a global agreement or a world court, stay tuned for battles between disclosure and privacy. If you're European, you have rights greater than those available to American citizens in having certain information about you deleted. But wherever you live, remember, protecting your personal data starts with you.

For more information, please contact [Joe Dehner](#) or any attorney in Frost Brown Todd's [Privacy and Information Security Law Industry Group](#).

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.