Decision in Europe: Controversial Revival of Practical Obscurity

Implications of the Google Spain Case

May 20, 2014

By: Robert Gellman and Pam Dixon

On May 13, 2014, the European Court of Justice decided an important case involving privacy and search engines. The decision may have enormously broad implications for privacy, for search engines, and for the Internet as a whole. At this point, we can only speculate about those implications.

Let's begin with the facts. A Spanish citizen brought a case, objected that entering his name in Google's search engine produced links to legal notices in an online Spanish newspaper about his debts dating back to 1998. The debts had been long since resolved. The citizen complained both about the newspaper and about Google's providing the link when his name was searched. The Spanish courts rejected his request that the newspaper remove or alter the old story.

It was only the second part of the complaint that went to the European Court of Justice, the highest court for European Union law, for resolution. The complainant asked that Google Spain be required to remove or conceal the personal data relating to him so that the links to the newspaper no longer appeared in the search results. The Court upheld the request, making a number of novel and sweeping holdings.[1]

---

[1] *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Court of Justice of the European Union (13 May 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=129807,

Key Aspects of the Court's Decision

First, the Court held that by searching systematically for information published on the Internet, the operator of a search engine collects personal data within the meaning of the EU Data Protection Directive. The operator's collection and related activities qualify as *processing* under the Directive even though the information had already been published elsewhere by others Thus, the search engine is the *data controller* for its processing of the data.

Finding that a search engine is a data controller is a big deal. It means that the European Union Data Protection Directive applies to the search engine, and the search engine must comply with the responsibilities assigned to all data controllers. A search engine can no longer claim that it is just passively reporting on information collected and made available by others. It must take responsibility for its own processing of personal information. This is a significant change from what was the status quo.

Second, the Court found that Google Spain is an establishment in Europe, so that the EU Data Protection Directive applies to it, along with all of its substantial privacy protections. Google's argument was that the processing actually took place elsewhere, but the Court rejected the argument. Google Spain sold advertising to support the search facility, and the processing was accomplished in that context. This holding may greatly expand the application of the Directive to Internet processing generally.

As we continue to describe further parts of the decision, note that the Court descriptions of the consequences of its findings are not absolute. We've highlighted the major *weasel words*.

Third, because Google is a data controller subject to the EU Directive, Google must, *in certain circumstances*, remove links to third party webpages that have information from results based on a search by an individual's name. The search engine's obligation to remove a link applies even if the original publication is lawful. Why? Because the information concerns aspects of the individual's personal life that would not be available (or only with great difficulty) without the search engine. It is the search engine that allows creation of a more detailed profile.

The Court took note of the importance of search engines in modern society in making information available to all. No matter what you think of the rest of the decision, it's hard to deny that point. The next step is more controversial The Court went on to find that neither the economic interest of the search engine nor the interests of Internet users was sufficient to outweigh the interests of data subjects. However, the Court also observed that the balances involved depend, *in specific cases*, on the sensitivity of the information for the data subject's private life, the interest of the public in accessing the information, and the role played by the data subject in public life. In other words, public figures may have diminished ability to protect their privacy.

Finally, the Court concluded that the Data Protection Directive enables a data subject to ask that links be removed from search engine results *after a certain time* if including the links is *incompatible* with the Directive. Regardless of the initial lawful and accurate publication, data may have become *inadequate, irrelevant, or excessive in relation to the original purpose*. The

judgments required here are not simple, and it falls on the search engine to accept a data subject's request and rule on its merits.

Implications of the Ruling

The European Court's judgment is not subject to further appeal, and we can assume that it is final. If so, what are the implications? We could probably write all day, but we will limit our comments to a few points.

Ruling may have wider reach

Until now, search engines have avoided privacy responsibilities as data controllers under the privacy regulations. The court focused on take down notices, but the ruling may go further. Carrying out the Court's order may now prevent search engines from providing the same search results to users in Europe than they provide to users elsewhere. It may also have other implications regarding implementing other parts of the privacy regulations. It's unclear just how far this will go in changing the general privacy obligations of search engines.

Challenges and expense of implementation

Search engines will have to make decisions on "take down" requests by an unknown number of individuals. Responding to requests will be neither simple nor inexpensive. There will need to be rules and procedures for handling requests, and the Court's vague standards for taking links down will need to be fleshed out. Some search engines may conceivably stop doing business in Europe to avoid takedown obligations. For individuals, making a takedown request for a link at Google may just be the start of a long process, for example, an individual may have to make the same request at Bing, DuckDuckGo, and dozens of other search engines. Different search engines might rule differently on the same request. We speculate that a central takedown service might eventually arise.

Other Internet companies

The Court's decision may bring within the scope of the Data Protection Directive other processing activities performed by other Internet companies in other countries for users in the EU. How many US companies that do business over the Internet will now fall directly under the Data Protection Direction? This is far from clear, but we observe that consumer privacy protections under the Directive are usually broader and better than protections under US law.

Pressure to redraft the Directive

The EU is currently debating changes that would turn the EU Directive into an EU Regulation. One of the major points of debate has been over a proposal to add a *right to be forgotten*. The debate is too long and complicated to summarize here, and the outcome of that debate and of the right to be forgotten remains uncertain. However, what the European Court did was to find a right to be forgotten in the current Directive, something that no one really thought was there. On

this point – as well as on the major findings and conclusions of the Court's decision – the debates on the proposed new Regulation will take a major new turn. There is likely to be enormous pressure to redraft the Directive to overturn some or all of the decision. This is likely to delay progress on the new Regulation, perhaps for a long time. On the other hand, perhaps the business community that opposes the new Regulation will conclude that overturning the Court's decision is a reason for action.

Revival of practical obscurity

Finally, we titled this note *The Revival of Practical Obscurity*. In Department of Justice vs. Reporters Committee,[2] the US Supreme Court decided a Freedom of Information Act (FOIA) case involving disclosure of criminal history records ("rapsheets"). The FBI centralized rapsheets for individuals by collecting records from federal and state law enforcement agencies. A reporter requested the rap sheet of a particular individual. All of the information in his rapsheet was presumptively public in police stations and court houses throughout the country. Nevertheless, the Court found that the centralized records were exempt from disclosure on privacy grounds under the FOIA. The decision turned on the *practical obscurity* of the records in their original location. In other words, even though the material was presumed public, in truth the materials were in practice difficult to obtain. That obscurity protected privacy, and the privacy interest overcame the public interest in disclosure.

The 1989 case was and remains controversial on its own. Over time, however, the Internet has almost completely destroyed the notion of practical obscurity. Much personal information that once disappeared from public view entirely or that was only accessible in dusty paper or microfiche newspaper morgues or government offices in State Capitols is now available online. Search engines are one of the tools that destroyed practical obscurity as a…sorry…practical matter.

The new decision by the European Court of Justice revived practical obscurity, something that was largely unexpected. The Court recognized the central role of search engines in modern life, and search engines will now have some accountability for addressing personal privacy. Personal data can become too old and too irrelevant to allow further processing or disclosure. Search engines can no longer claim that they are mere conduits for information maintained by others, which changes much, and with unknown long-term impacts as of yet.

Some Conclusions

In closing, we offer a few final thoughts about the decision. We suspect this ruling will have unintended consequences that have a long reach, and the consequences may be both beneficial and deleterious to any number of parties simultaneously. It is a decision with much unknown impact and much complexity.

[2] 489 U.S. 749 (1989), http://supreme.justia.com/cases/federal/us/489/749/case.html.

First, it seems unlikely that any court in the US would reach a similar result. Not only do we have no privacy law similar to the EU Directive, but we also have a powerful First Amendment that protects free expression.

Second, it may be years before the consequences of the EU Court's decision are fully understood. In the meantime, there will be enormous additional resources devoted by Internet companies to lobbying on the EU Regulation, much litigation, and many interesting new law journal articles.

Third, an individual seeking to implement the right that the European Court recognized may find it so difficult to do that, perhaps, the decision creates the idea of *impractical* obscurity.

Fourth, search engines may take down links when individuals object. The actual links may remain as they were, still accessible if you can find them. Thus, a search engine may have access to suddenly obscure personal data that others cannot readily find, which is both intriguing and disconcerting. How will law enforcement, national security, and anti-terrorism agencies respond to the new limits? (Including government requests from other countries?) This issue area may prove to be fertile for unexpected consequences.

Finally, we think that the decision is mostly good for privacy but more of a mixed result for the Internet at large.

These are not simple or easily-reached judgments, and we consider them to be tentative. Many different interests are at stake here, and privacy is just one of them. Privacy appears to have won the first round in this battle, but there will be many more rounds to come in other cases and other places. It will be important to watch how the decision is implemented down the road and to conduct research on who are the primary take-down requesters over time. (Bad actors? Vulnerable populations? Others?) There will be no shortage of things to discuss.

About the World Privacy Forum

The World Privacy Forum is a non-profit public interest research and consumer education group focused on the research and analysis of privacy-related issues. The Forum was founded in 2003 and has published significant privacy research and policy studies in the area of health, online and technical, privacy, self-regulation, financial, identity, and data brokers among other many areas. www.worldprivacyforum.org.

About the Authors

Robert Gellman Robert Gellman is a privacy and information policy consultant in Washington DC. (www.bobgellman.com.) He has written extensively on health, de-identification, Fair Information Practices, and other privacy topics. Dixon and Gellman's writing collaborations

include a reference book on privacy Online Privacy: A Reference Handbook, as well as numerous and well-regarded privacy-focused research, articles, and policy analysis.

Pam Dixon is the founder and Executive Director of the World Privacy Forum. She is the author of eight books, hundreds of articles, and numerous privacy studies, and is co-author of many privacy studies with Robert Gellman. She has testified before Congress on consumer privacy issues as well as before federal agencies.

Document Information:

Publication date: May 20, 2014
At www.worldprivacyforum.org
v. 1
Any updates to the document will be posted at www.worldprivacyforum.org.