Stanford Law School

Daphne Keller
Director
Intermediary Liability
Stanford Center for
Internet and Society

Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
Tel 650 723-1417
daphnek@law.stanford.edu

January 23, 2018

Comments on the Guidelines on Transparency under Regulation 2016/679

To the Honored Members of the Article 29 Working Party:

1. I write as the Director of Intermediary Liability at Stanford Law School's Center for Internet and Society. My work there has focused closely on the "Right to Be Forgotten" or "Right to Be De-Listed" under EU data protection law, and under the GDPR in particular. I previously served as Associate General Counsel for Google. In that capacity I worked closely with, and learned a great deal from, Google's Advisory Council on the Right to Be Forgotten and the numerous experts who shared their insights with the Council.

2. My comments on the Draft Guidelines on Transparency under Regulation 2016/679 are brief and focused solely on the issue of Internet intermediaries. They reflect the closer legal analysis of GDPR transparency provisions in my forthcoming Berkeley Technology Law Journal article, *The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation*. The full article is attached to this communication and is available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914684.

3. Applying data protection law to Internet intermediaries raises complex issues relating to the legal and fundamental rights of Internet users – including rights under Articles 7, 8, and 10 of the Charter of Fundamental Rights of the European Union. These issues are discussed at a high level in section II.C (*Data Protection and Online Service Providers*) of the article, and have also been addressed in important work by European scholars.[1] A pending case before the CJEU – in which Google and the French Data Protection Authority

[1] *See*, *e.g.*, Jef Ausloos and Aleksandra Kuczerawy, *From Notice-and-Takedown to Notice-and-De-List: Implementing the Google Spain Ruling* (2016); David Erdos, *Beyond 'Having a Domestic'? Regulatory Interpretation of European Data Protection Law and Individual Publication* (2016); Miquel Peguera, *The Shaky Ground of the Right to be Delisted* (2016); Brendan van Alsenoy, *The Evolving Role of the Individual Under EU Data Protection Law* (2015); Joris van Hoboken, *The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment* (2013).

both seek the same outcome regarding a specific set of delisting decisions – will soon provide clearer guidance on them. In the interim, the Article 29 Guidelines can set parameters to better protect the rights of all concerned, and to better guide Internet companies seeking to comply with the law with regard to the narrow but important topics listed below.

Special Concerns of Data Subjects Who Post Information on Social Media or on Sites Indexed by Search Engines

4. GDPR Articles 12, 13, and 14 contain provisions that appear generally reasonable with respect to data, such as ad profiling information, collected and used by Internet companies at the "back-end" of their services. The same provisions may have unintended and harmful consequences, however, if applied too literally to another class of data: information publicly posted online by Internet users themselves.

5. Consider a situation in which Data Subject A posts information about Data Subject B. This could, for example, be an employee tweeting that a senior manager at her company does poor or error-riddled work, or posting the same allegation as a comment to a news article about the company. Under current law, Google or another search index that made this comment available in search results would be deemed a controller with resulting obligations to Data Subject B, the manager. It remains to be seen whether a social media hosts such as Twitter or Facebook might also one day be deemed the controllers for such information.[2]

6. Online controllers' obligations to Data Subject A – as the author of the post – are comparatively straightforward. Obligations to Data Subject B – the person being discussed – are less so. As discussed in section III.C.4 of the article, the GDPR appears to create obligations toward Data Subject B that are seriously at odds with Data Subject A's interests and fundamental rights. It is my belief that the most extreme of these apparent obligations were not intended by GDPR drafters. Nonetheless, without guidance from the Working Party, entities unclear on their legal duties may act upon them.

7. Under Article 14.2(f), the controller is instructed to tell data subjects – in this case Data Subject B, the manager – "from which source the personal data originate." Article 15.1(g) further requires the controller to provide "any available information as to [the data's] source[.]" On their face, these provisions appear to require a controller to tell the manager information about his employee – potentially including things like a personal email address linked to her account, the time and IP address corresponding to the post, or even content of her other online communications. This could obviously burden not only on the employee's own data protection rights, but other fundamental rights.

[2] Legal complexities of this question are discussed in section III.B of the article, *Right to Be Forgotten Obligations for Hosts and Social Media*.

8. A related set of concerns around improper data disclosure arises when a data subject exercises rights under Articles 17 and 21. Objections and erasure requests trigger obligations for the controller to further disseminate information about the data subject's requests. Here again, the GDPR's rules seem well-considered for "back-end" data processing and sharing among corporate and institutional controllers. But they risk serious unintended consequences as applied to information shared on Internet platforms by members of the public.

9. The GDPR requires controllers to communicate information about such requests to "recipient[s] to whom the personal data have been disclosed" (Art. 19) and other "controllers which are processing the personal data." (Art. 17.2) For a search engine honoring a de-listing request, this could mean communicating it to the webmaster who originally posted the information – despite the Working Party's position that such notice is usually improper. It could also, for search engines or other platforms, mean communicating the request to other account-holders known to have viewed, liked, commented on, or shared the information. Such disclosure would in many cases go against the interests of the data subject and strip him of power to, in the Working Party's words, "choose how to exercise" his rights by "selecting one or several" among possible recipients for objections or erasure requests.[3]

10. As discussed further in the article, there are possible grounds for exceptions to, or alternate interpretations of, these provisions. However, the interpretations listed here are the simplest and most obvious, particularly for intermediaries that lack European counsel. The Working Party could avoid considerable uncertainty and potential harm by clarifying protections for all data subjects under these portions of the GDPR.

Transparency About Search Engine De-Listing Standards

11. A second issue, also addressed in the section III.C.4 of the article, involves transparency to the public or researchers about standards applied by companies de-listing search results. If social media hosts such as Facebook or Twitter are deemed controllers for individuals discussed in a third party's posts – like Data Subject B, the manager, in the example above – similar transparency and accountability concerns will arise. This issue is a complex one and likely outside the scope of the Working Party's current draft Guidelines. However, the current Guidelines could include a placeholder, or be drafted so as not to preclude later guidance on this important topic.

12. Researchers from civil society, academia, and government have long expressed frustration at the "black box" of company decision-making under *Google Spain*. Without better information, many charge that companies remain unaccountable and that the process lacks sufficient public legitimacy. This concern is particularly acute for those cases in which a platform improperly *accepts* a de-listing request (as opposed to improperly *refusing* to

[3] *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales* at 7, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

de-list). Those cases, in which the data subject achieves his de-listing goal, are less likely to be reviewed by DPAs or other appropriate authorities. As a result, errors caused by a controller's mistake or lack of familiarity with regional public interest issues are less likely to be identified and corrected.

13. For search engines and other potential controllers, of course, the further transparency sought by civil society is the subject of legal concerns. Sharing more precise or granular information about de-listing standards in difficult cases might risk disclosing personal information about the data subject, bringing both legal penalties and public opprobrium to the company.

14. This impasse is frustrating to both sides – public researchers and the private companies they wish to research. Solutions that adequately respect both transparency principles and the fundamental rights of all concerned are as yet unclear.

15. What is clear, though, is that data protection authorities, and the Working Party in particular, are uniquely well-positioned to help remedy this situation. Future Working Party Guidelines could, for example, approve disclosure of particular classes of information, or approve limited data sharing with academic researchers, subject to clear restrictions on usage and disclosure. Thoughtful and narrowly tailored transparency provisions, developed through consultations with experts on all sides of the issue, would support fundamental rights and the fairness and accountability principles of the GDPR.

Respectfully submitted,

Daphne Keller
Director of Intermediary Liability
Stanford Law School Center for Internet and Society