THE RIGHT TO BE FORGOTTEN

ABSTRACT

The European Court of Justice's (ECoJ's) ruling on what is now known as the 'Right to be Forgotten' sets a clear direction of travel and brings some important points into focus. Suggesting, as some have, that this ruling is a new form of censorship is certainly incorrect. The Right to be Forgotten is an important personal right and the ECoJ has made it clear Data Controllers are required to give people the ability to exercise it. However, I do believe the ruling exposes an imbalance in current Data Protection legislation that warrants attention. I also believe it raises the bar for all organisations that put people's personal data online. Assuming national Information Commissioners give the ruling teeth, it will require all Data Controllers, not just search engine operators, to review and update their privacy practices in non-trivial ways.

This article relates to the ruling made by the European Court of Justice on 13 May 2014. It starts by describing the essential points from the ruling. It then explains two important issues this ruling brings to light along with their potential ramifications.

THE ESSENTIAL POINTS FROM THE RULING

In 2010, an individual in Spain asked a local newspaper to remove personal details relating to him from two articles it had published in early 1998. He also asked Google Spain and Google Inc. to remove links to those two articles from the results of any searches made against his name. His reasoning was that the matter mentioned in those articles had been fully resolved and any further reference to them was outdated.

The Spanish Data Protection Agency (AEPD) took the view that the newspaper had published his personal data lawfully and did not need to take the requested action. It did uphold the request against Google and instructed Google to render access to the articles impossible in the future. Google challenged the AEPD and this led to the Spanish High Court referring the matter to the European Court of Justice (ECoJ) for a decision.

The ECoJ found that:

- Search engine (SE) operators collect, organise and disclose data and, as such, they fit the role of Data Processor for any personal data caught up in the results of a search. That the personal data has already been published on the internet by a separate Data Processor (in this case a publisher) has no bearing. SE operators perform additional processing to that performed by publishers and to that extent are Data Processors in their own right.
- SE operators determine the purpose and means of the processing they perform. Therefore they are Data Controllers for any personal data they process.
- As a consequence of these roles, SE operators within Europe are obliged to comply with relevant Data Protection principles and legislation. They are not covered by any exemption that relieves them of this.
- By aggregating data from many available sources and presenting them to a user in an ordered form, a search engine can provide a user with a potentially detailed profile of another person that that user could not have obtained by other means other than with great difficulty. It is this

creation and provision of a detailed profile that constitutes interference with that other person's right to privacy and potentially gives that person the right to seek redress.

- Accurate data can, with the passage of time, become outdated, i.e. no longer relevant to the original purpose for which it was published. Data can also, with the passage of time, become inadequate, irrelevant or excessive with respect to the original purpose. Such data is, as the ECoJ puts it, "*incompatible with the Directive*" (by which it means EU Directive 95/46/EC – the EU Data Protection Directive).
- Directive 95/46/EC gives Data Subjects the right to request that data that has become 'incompatible' be 'forgotten', and the ECoJ upheld this. It did acknowledge one caveat: that internet users also have legitimate interests that might be satisfied by SE searches, and that 'incompatible' data must be 'forgotten' "*unless there are particular reasons, such as the role played by the Data Subject in public life, justifying a preponderant interest of the public in having access to the information*".
- A Data Subject has the right to request 'incompatible' data be 'forgotten' simply on the basis of the data being incompatible. He/she does not need to show that retention of that data would (or might) cause them harm or prejudice.

The ECoJ ruled, for the particular case before it, that Google must remove links to the outdated data as requested by the Data Subject. Google was required to do this even though:

- The outdated data, when originally published, had been published lawfully.
- The publisher was not put under any equivalent obligation to remove the data, even though the data had become outdated.

The publisher was not required to remove the data because publication made "solely for journalistic purposes" benefits from an exemption under the Directive. Processing by a search engine was not performed solely for journalistic purposes and was not covered by that or any similar exemption.

TWO ISSUES THIS DECISION BRINGS TO LIGHT

This is a significant decision that brings into focus a number of important points. I have no doubt that the judgement is legally correct. However, I believe it exposes an imbalance in current Data Protection legislation that warrants attention. I also believe it raises the bar for Data Controllers. Assuming national Information Commissioners give the judgement teeth, it will require all Data Controllers (not just SE operators) to review and revise their privacy practices.

Though the ruling was made against Google specifically, we can presume it applies as a general ruling to all SE operators operating in the EU. Indeed, I see no reason why it should not apply to all Data Processors and Data Controllers that do not benefit from a relevant exemption under the Directive.

My view of the ECoJ decision is this.

- Search engines do perform significant processing. They do more than just point the user to relevant data available on the internet. They process that data – they aggregate it, assesses it for relevance and present it in an organised form. The aggregation and organised presentation of data from a wide variety of sources adds significantly to the sum of the individual components that would otherwise remain dispersed and more difficult to locate. SE operators cannot claim to be 'just the messenger of other people's data'. ISPs might well be able to use that defence but SE operators cannot.

- Search engine results can present a significant interference with a person's privacy. Search engine results, in and of themselves, constitute an additional interference over and above any interference caused by the original publication of each constituent part of that person's data. Furthermore, that interference can be significant.
- We should all be able to insist that the processing of our personal data must be fair and lawful and must not unjustly harm our interests or interfere with our rights. For a search engine to present outdated data alongside accurate and current data with nothing to indicate that any of that data is outdated or in any other way inaccurate or incomplete can reasonably be considered unfair. Mechanisms should be in place to allow us to defend ourselves from this type of unfair processing.
- The issue is not whether we as individuals have the right for some classes of personal data to be forgotten – it is clear that both morally and legally we do – but who has what responsibility for enabling us to exercise that right.

Up to this point, I am comfortable with the ECoJ's reasoning. However, I now start to diverge from them. In particular, I think the ECoJ's judgement exposes an imbalance in current Data Protection legislation that warrants reconsideration.

The ECoJ did not require the publisher to remove outdated data it had previously published. It recognised that data that had been originally published lawfully can become outdated or otherwise 'incompatible with the Directive' but did not require the publisher to do anything about that. This is primarily because publishers who publish under one of the small number of 'special purposes' identified in the Directive (*journalism*, *art* and *literature*) are exempt from many of the requirements of the Directive. Article 9 of the Directive gives publishers exemption:

- If they are publishing solely for one of the named 'special purposes', and
- If they believe that publication is in the public interest.

This exemption is a 'Get away with anything' card for media publishers. Provided they claim that publication is in the public interest, they are exempt from the Directive's requirements to ensure that the information, at the time they publish it, is correct, accurate, complete, current and proportionate. In addition they are not required to adjust that information at any later stage if it becomes incorrect, inaccurate, incomplete, outdated or excessive.

The ECoJ is alert to the need to achieve a fair balance between competing interests (in the case before it these were the interest of the Data Subject and the interest of the SE user) and did allow that an SE operator would not have to remove links to 'incompatible' data if there were "particular reasons ... justifying a preponderant interest of the public in having access to the information". However, it was of the opinion that, for the case before it, no such particular 'public interest' reason existed.

As a result, we find ourselves in a contrary situation. There are not sufficient public interest reasons to allow the SE operator to retain links to outdated personal data but there are sufficient public interest reasons to allow the publisher to exercise the 'journalism' exemption available to them and not be obliged to make any amendment where personal data has become outdated. This does not sit well with me.

I understand why the ECoJ ruled as it did. However, I do believe that a 'public interest' defence should work equally for all who want to rely on it, and that the level of the bar should not be set lower for media companies than for others. A fair balance should place the responsibility for removing outdated (or otherwise 'incompatible' data) on the original publisher before it should be placed on the SE operator. I offer four reasons in support of this view:

- The SE operator was not responsible for putting the personal data in the public domain in the first place, the publisher was.
- Though media companies are prone to putting themselves in an exalted role as protectors of the public's right to know, publishers are profit-making companies operating for their own commercial interests just as much as SE operators are.
- The publisher knows the original purpose for which the data was published and is better placed than any SE operator to judge at what point data becomes no longer relevant, accurate or complete for that purpose.
- It does not follow that the responsibility for 'forgetting' data should fall to SE operators simply because they tend to be good at putting relevant data in front of an interested user. That a publisher might find it hard to make relevant material they published a long time ago easily located by the interested user whereas search engines tend to be good at it should not relieve the publisher from its responsibility to respect a person's right to fair processing.

This leads me to the view that the 'special purpose' exemption in current Data Protection legislation is not balanced. I would be pleased if one of the consequences of this ECoJ ruling is that this imbalance receives renewed consideration and is revised.

The second issue I believe this ruling raises is a matter for all Data Controllers.

This ruling by the ECoJ shows that people can expect to be supported by the courts if they exercise their right to challenge the way their personal data is used. People need to show only that the processing being performed is 'incompatible' with applicable Data Protection legislation, not that continued processing would (or even might) cause them harm or prejudice. Several tens of thousands of people have already, within one month of the ruling, submitted requests to Google to have 'incompatible' data about them be 'forgotten'. This level of immediate take-up suggests that people do object strongly to unfair processing and such challenges could well become a common feature of the Privacy landscape.

This raises the bar for every organisation that processes or puts anyone's personal data online. Not only for Google, and not only for SE operators, but for every organisation that is not able to use the 'Get away with anything' card granted to those that publish under one of the Directive's special purposes. This is because any non-exempt organisation in receipt of a 'Right to be Forgotten' (RtbF) request from a Data Subject will be expected to have the procedures in place to enable it to respond to that request and make the right decision on their use of the Subject's data even if they are not the original source or processer of that data.

Organisations will find this requirement more difficult to satisfy than satisfying SARs (Subject Access Requests). In the case of SARs, all the information the organisation needs to enable it to fulfil the request is located within the organisation. No third party needs to be involved. For an RtbF request, that is not the case. In simple cases, and the case involving Google was a relatively simple case, the recipient organisation might well be able to make a reasonable decision on its own. In many other cases, the organisation will need to get the original source or processor of that data involved. It will need that third party to furnish it with relevant data relating to the purpose of their original processing. It will also want to offload responsibility for making the decision on to the original processor so it can alleviate itself of any potential liability.

In a world where Data Subjects feel empowered to make RtbF requests, everyone who processes or puts anyone's personal data online will need to rethink their practices.

- Firstly, organisations will need to recognise more than they might have done in the past that they have an ongoing responsibility for the data they put online and to the Data Subjects they cover.

They are responsible for ensuring the data is accurate, current, complete and proportionate when they put it online, and remains so for the entire period that that data is online. 'Publish and forget' is no longer viable in a world where Data Subjects have an exercisable Right to be Forgotten.

- Organisations, if they are to respond efficiently and within a reasonable period to RtbF requests, will need to keep better track of the data they put online. They will need to record the purpose for which it was put online originally and the criteria the data needs to satisfy if it is to remain 'compatible'. That will include assigning a retirement date for each type of personal data they process.
- The larger the organisation and the larger the number of Data Subjects whose data it processes, the more the organisation will need to deal with 'incompatible' data automatically and proactively rather than manually in response to each RtbF request it receives. Larger organisations will need to develop practices and procedures that ensure they record the purpose, criteria and retirement date for all the personal data they process at the time they put it online. They will need a practice for assessing the data periodically against the criteria recorded so if the quality of the data degrades for any reason (it becomes outdated, circumstances change, events require it to be updated, etc.) they can respond accordingly.
- Any organisation that takes personal data from an online source and processes it further will need to develop procedures for finding out from original sources what the purpose and criteria associated with the data are so they can respond correctly to the RtbF requests they receive.

Organisations will find that putting the Right to be Forgotten into practice will not be simple and will need them to rethink their personal data practices. Individuals will also be affected. Users of social network sites who post data about people they know will also, in theory, be subject to this decision. As it is unrealistic to think of enforcing Data Protection principles and redress procedures on vast numbers of individual social network users, it is the social networking sites themselves that will have to set up default practices that fulfil this responsibility on behalf of their users. For example:

- Operators of social network sites might have to implement a default that causes individual people's postings to expire after a set period of time, say ten years, on the basis that almost all such postings will be outdated by then.
- They will be required to act on requests from Data Subjects to remove 'incompatible' postings where the original poster has failed or declined to do so.

  And here I can see value in the ECoJ's ruling that a Data Subject can ask the operator to remove the outdated posting without having to ask the poster beforehand or in parallel. That could save millions of people having to make RtbF requests to millions of former or current friends and in the process reminding their friends of the reason they feel injured by the content of their original post.

The Right to be Forgotten is an important right and people need to have the means to exercise it. Though it might be a long time before we reach the stage where RtbF requests are routine and all large organisations have competent practices, I think the direction of travel established by this ECoJ ruling is clear. Putting people's personal data online has just become more challenging.