EU INTERNET REGULATION AFTER GOOGLE SPAIN

3/27/15

Report of Proceedings

UNIVERSITY OF CAMBRIDGE

Centre for European Legal Studies
Faculty of Law
University of Cambridge

INTRODUCTION

The Court of Justice of the European Union's May 2014 decision in *Google Spain* (C-131/12) finding that Google search engine must be deemed a controller under Spanish data protection law and that individuals had the right to demand erasure of data in certain circumstances (the so-called "right to be forgotten") sent shockwaves across the internet policy community. It also prompted by far the most high-profile public debate to date on data protection and the challenges which it faces, notably as regards the need for a balance between competing rights and interests on the internet and how to ensure effective enforcement in an ever more complex and globalized technological environment. Much of this public debate focused solely on the justifiability or otherwise of granting individuals a limited erasure right against search engines. Nevertheless, even this discussion highlighted the profound consequences of this case for future of the internet.

The idea of organizing a one-day conference pivoting around *Google Spain* arose out of a clear understanding of the judgment's central importance – both in terms of the development of legal doctrine and in terms of societal debate on data protection. At the same time it was recognized that, given the voluminous discourse and commentary which had already ensued, it was vital to ensure that the proceedings really added value. With this in mind, the Conference had five key aims:

- Firstly, we sought to explore the historical background to the judgment, couched, as it was, within a context within which data protection is, at least in Europe, increasingly seen as a fundamental right in and of itself. The implications of these development can be seen not only in *Google Spain* but also in other recent cases such as *Digital Rights Ireland* (C-293/12).
- Secondly, as regards the responsibilities of search engines specifically, we aimed to engage in a genuinely dispassionate and searching study of the key issues arising, drilling down into fundamental concepts and exploring the various aspects which remain contentious and/or unresolved.
- Thirdly, we also sought to explore the potential broader context of *Google Spain,* both as regards the data protection obligations of other internet actors (such as blogs, social networking and street mapping services) and as regards the thorny issues of applicable law and regulatory jurisdiction.
- Fourthly, and inter-related with the previous three aims, although developing from an academic base we sought to bring together a wide range of relevant actors including from the worlds of e-commerce, regulation, government and civil society.
- Finally, we sought to ensure that the conference ensured that it led to output – and notably this publication - which could act as a continuing resource for those interested in exploring further the interface between data protection, freedom of expression and the regulation of the internet.

I will leave it not only to the conference participants but also to you when reading these Proceedings to consider whether we were successful in our aims. However, whatever else, I and I think many others at the conference came away with the distinct feeling that this was in many ways the beginning not the end of a wide-ranging debate. Those of us engaged in information law here at the Faculty of Law at Cambridge look forward to continuing to engage with you in that debate in the years ahead.

Dr. David Erdos
Conference Convenor

CONFERENCE ORGANIZING COMMITTEE

Convener: Dr David Erdos, University Lecturer in Law and the Open Society and WYNG Fellow in Law at Trinity Hall, University of Cambridge

Administrator: Mrs Felicity Eves-Rey, Centre for European Legal Studies, Faculty of Law, University of Cambridge

Committee Members: Mr Oliver Butler

Dr Richard Danbury

Ms Ann Kristin Glenster

Ms Rebekah Larsen

Ms Julia Powles

ACKNOWLEDGMENTS

We would like to record our profound appreciation to **Hogan Lovells** for a donation which made this conference possible. We would also like to record our thanks to **Cambridge Big Data**, the University's Strategic Research Initiative in this area, for their financial contribution.

PRESENTATION SUMMARIES

SESSION 1: THE PATHWAY TO GOOGLE SPAIN

PROFESSOR ARTEMI RALLO LOMBARTE

Gave background to *Google Spain* citing Spanish cases.

- Where information has been published in the official gazette or in newspapers. In these cases the Spanish Data Protection Agency has ordered Google to erase a link but did not require the Gazette or the newspaper to delete the information.
- In Google Spain, the Spanish Data Protection Agency (and the CJEU) established that European law is applicable to search engines, and that the search engines are data controllers with independent responsibility from the webmasters.
- Unlike newspapers, search engines are not the subject of fundamental rights (freedom of speech). Their legitimate interest in processing is only economic.
- Information of public interest should not be subject to deindexing.
- The only difference between the Spanish Data Protection Agency and the CJEU ruling is that the CJEU emphasises that the right to erase is equal to the right to object because the passing of time alters the meaning of information.
- In its actions leading to Google Spain, the Spanish Data Protection Agency did not have many allies even amongst fellow EU Data Protection Authorities.

JEF AUSLOOS

- Raised a need to clarify the conceptual issues as memory cannot be not erased with a 'right to be forgotten'. Instead, he outlined specific concepts related to this debate including the *droit à l'oubli*, right to erasure, right to object, and right to be delisted.
- Personal information is often not either completely public or private, but exists on a continuum of practical obscurity.
- Search engines are not neutral in their presentation of data. Their algorithms produce particular search results.
- Search engines should only be the starting point for investigative journalism.
- As regards the debate on giving original publishers 'a voice' as regards deindexing, some publishers are more legitimate than others and, in any case, it is not clear that publishers have a right to be indexed.

DR ORLA LYNSKEY

- Reviewed the CJEU jurisprudence leading to *Google Spain* arguing that the history of cases is generally consonant with the Court's findings.

- The Court has consistently insisted on broad scope of application of the Data Protection Directive.
- The Court is placing increasing emphasis on EU Charter Articles 7 and 8.
- The Court is emboldened and not overly concerned with the potential political fallout and appears somewhat indifferent to the disconnect with new technological development.
- The definition of journalistic purposes has narrowed with *Google Spain.*

SESSION 2: THE CHANGING LANDSCAPE FOR SEARCH ENGINES AFTER GOOGLE SPAIN

WILLEM DEBEUCKELAERE

- *Google Spain* is not only about the right to be forgotten, but about power in general.
- Some may find it difficult to accept the ruling because previously privacy and data protection has been considered only as an interest, but it is clear now that it is a fundamental right.
- The Article 29 Data Protection Working Party was surprised that the Court stated that the "right to be forgotten" was a fundamental right on the level of a human right.
- The Article 29 Working Party was concerned that *Google Spain* would open the floodgates for applications to the Data Protection Authorities. However, the Data Protection Authorities also felt empowered by it.
- EU DPAs met frequently with Google and the Article 29 Working Party sought to devise a common position for all EU states resulting in Guidelines which outline thirteen criteria for evaluating potential deindexing.
- The most important outstanding question relates to the territorial validity. Google has accepted this is a European law that should be implemented in the whole of Europe. However, it is also a personal right which suggests that it maybe should apply worldwide.
- The biggest feared problem for the Data Protection Authorities was censorship.
- The lesson to be learned from *Google Spain* is that the Data Protection Authorities must be brave like the Spanish Data Protection Authority.

WILLIAM MALCOLM

- Google respects the *Google Spain* decision and has worked to give it effect.
- According to the Google Transparency Report, as of 23rd March 2015 Google has received 843,000 individual delisting requests, of which less than 41% were delisted. This represents quite a volume of work for the company.
- The first thing Google did following the ruling was set up a system to respond to requests through a web form focused on EU users.
- Google deindexes from EU and EFTA domains. Despite the judgment focusing on national removals, Google has taken a pan-European approach. Google does not remove links within non-European sites, including .com, as Google does not see the Court's ruling as global in its reach.
- Google is also focused on transparency. Google informs the webmasters if a link is removed, and will evaluate complaints and may reinstate links.

- The CJEU criteria for removal are vague, so Google has developed more detailed criteria, and welcomes further Article 29 Working Party guidance.
- Some big areas of contention for delisting relate to public figures, news stories and political speech.
- Some Data Protection Authorities have asked Google to remove government records, and in some instances asked to remove in complex defamation cases.
- Different standards are applied by different Data Protection Authorities' as regards certain requests for removal, particularly in relation to past criminal records.
- Google does not draw hard lines, but takes a dynamic approach and looks at a range of factors.

JULIA POWLES

- Google Spain raises issues of informational power and privacy in a surveillance-based economy.
- The issues are not clear as the hundreds of thousands of requests being made to search engines range across the full spectrum of human experiences, but Google has publicly only has not revealed the necessary granular information to move beyond the general and to the particular. This lack of transparency exacerbates misunderstandings and promotes ideological and intercultural conflict.
- There is an issue with representation, as the bulk the requests for delisting appears to be from people with a low public profile, in contrast to the media personalities and others who discuss the right to be forgotten. There is also a gender imbalance in that most of the participants in debates are male.
- *Google Spain* is an externality of three deeper issues: the vast informational power held by search engines, the fundamental tension between the aspirations of European data protection law and the capacities and expectations of internet users, and thirdly the surveillance-industrial complex.
- Internet companies have made us believe the internet is a public space when it is in fact a representation of privately owned services. Google's dominance has created asymmetries of power.
- A discussion of intricacies and inadequacies of European data protection law, such as around treatment of sensitive data or around national implementation, has been missing in this debate.
- This may be the first time the general public appreciates the reach of European data protection law.
- The *Google Spain* decision is an essential litmus test for meaningful data sovereignty rights.

EDUARDO USTARAN

- Following *Google Spain*, search engines are now required to take down requests on the basis of the right to erasure.
- Whereas personal data and processing can be absolute concepts under the Data Protection Directive, the definition of the data controller depends on an intention to process information. However, in *Google Spain*, the Court took a broad purposive approach of interpretation thereby, by implication, turning the search engines in effect into super-controllers. No one has publicly recognised this implication.
- The determination of the applicability of law is also problematic. This Court's judgment implies that the local establishment criterion applies to a data controller established including in the EU, which would suggest that many EU-based controllers would have to comply with the laws of several countries.

- With Google Spain, the CJEU has extended and created the greatest extension of European data protection law ever attempted, changing the landscape for everyone.

SESSION 3: THE GENERAL SHAPE OF EU INTERNET REGULATION AFTER GOOGLE SPAIN

DR DAVID ERDOS

- *Google Spain* largely solidifies the dominant data protection paradigm with serious implications for almost every type of internet actor.
- There is a huge gap between the expansive interpretive stance especially of DPAs, and enforcement, which has been limited and sporadic.
- The dominant interpretative paradigm is composed of four key pillars: first, the key terms of the Directive have an extremely broad scope, and exemptions are exhaustive and extremely limited. Second, special journalistic and other purposes are in no sense unbounded. Third, there is a recognised need to balance data protection with other rights and the general principle of proportionality even outside the special purposes. But this is unclear as the fourth pillar is that data protection norms are often overriding, such that no explicit balance with freedom of expression is considered warranted.
- The paradigm outlined apparent especially in the attitude of most Data Protection Authorities, and every online media actor is in principle affected by this paradigm.
- This assertion was empirically tested through a survey in the European Economic Area with an 80% response rate from national data protection authorities.
- However, as regards enforcement, approximately 25% of DPAs responding to the survey confirmed that they had never taken enforcement action against online media expression under the Directive, and nearly 50% had not taken extensive action.
- Resources are mismatched to the task set for DPAs. It appears that DPAs have on average only approximately €0.30 to spend per resident data subject.
- It is dysfunctional to have a situation where the interpretive stance of regulators is at such variance with the practice in terms of how that is in reality enforced. This will only begin to chance if we have a debate about the dysfunctionality and costs for the rights people think they have and for the responsibilities that controllers might have.

DAVID SMITH

- The ICO responds to the issues that present themselves on a case-by-case basis.
- The crucial thing for the ICO was that the Court decided that Google is a data controller.
- This leaves a legal quandary especially as regards sensitive data.
- 200,000 people have complained to Google, nearly half have had the URL's removed and very few end up complaining to the DPAs. So a significant number of people are having their privacy concerns addressed.
- It is important to note the emphasis the Court placed on the EU Charter right to data protection (Article 8).

- It is not just the Court, but also the regulators, who are emboldened by *Google Spain* and the general direction of legal developments more generally.
- The Snowden case will have a real impact on internet regulation in the future.
- The case law is moving us from the Directive and closer to the future Regulation, so the latter will not be such a leap.
- The material scope of processing of personal data in the Regulation is huge.
- Consent cannot be the answer to every data protection problem as people are not in a position to make informed choices.
- The right to object in the Regulation is important because it shifts the onus of proof from the data subject to the entity processing the data, and that is a shift in balance.
- The exemptions for freedom of expression will be left to the Member States, with potentially significant differences in application, albeit perhaps with a greater consistency of approach than currently.
- Life is becoming more difficult for the DPAs, as seen with the *Rynes* decision which requires the regulation of the processing by individuals.
- Going through the consistency mechanism being drawn up in Brussels is becoming very complex, and there is a danger of a disconnect between the legislative scheme and reality. In the end, the focus should not be on legal niceties but on ensuring access to justice.

HUGH TOMLINSON QC

- *Google Spain* has an impact across all forms of internet services.
- Discussed *Vidal-Hall v Google*[1] as regards section 13 (2) of the UK Data Protection Act which seeks to restrict recovery of damages for moral distress absent economic loss being proved. Under the EU Charter's right to an effective remedy, this has now been disapplied.
- The UK courts are becoming more constitutionally aware due to the HRA and the EU Charter.
- As regards deindexing from search engines, what is to happen in not untypical cases when the data subject's concern is not with a single URL rather with masses of data all over the Internet? This issue was raised in the *Heggelin* case and is also being pursued by Max Mosley in relation to images.
- Google interprets the e-Commerce Directive as preventing courts from making proactive orders to block images or text. However, the e-Commerce Directive states that it does not apply to Data Protection.

JAMES LEATON GRAY

- From a media perspective, there are issues of imbalance with the Article 29 Working Party's suggestion that the publisher should not be informed about the removal of links. Debeucklaere said there was no issue with censorship, but how do we know that is true if the publisher is not informed that the link has been taken down?
- A danger of an absence of balance is also raised by DPAs being responsible for ensuring a balancing act between the right to data protection and freedom of speech. This is because they are set up to protect one of those rights and not the other.

- It is also problematic that a private company, however efficient and well-meaning, is being called to balance these rights as society does not have the resources to do this effectively itself.
- There is a disconnect between the law and reality and we are in danger of regulating and legislating in a silo separate from daily life. .
- The right to be forgotten applies to a range of internet players, not just search engines. One example is blog posts.
- In the not too distant future your news will be brought by algorithms and we may not know how the selection is being made, or what has been removed.
- The CJEU ruling was not balanced enough because it was based on a particular set of circumstances, where the freedom of expression was not sufficiently included.
- The proposed Regulation is based on old fashioned concepts and the harmonization that it proposes will make things more difficult.
- The Americans don't understand where we are coming from, and in a globalised world we are in danger of having a conversation with ourselves.

SESSION 4: JURISDICTION, APPLICABLE LAW AND BEYOND AFTER GOOGLE SPAIN

PROFESSOR DR JOHANNES CASPAR:

- *Google Spain* is of historical importance as search engines were seen as data controllers, and cannot escape European data protection law if they are established in at least one Member State country.
- The CJEU not only bolsters privacy rights, but also clarifies the scope of applicable national data protection law.
- The CJEU concluded that national data protection law applies if the activity of an establishment in the specific Member State is economically linked to the controller.
- Discussed regional litigation involving Facebook. Prior to *Google Spain*, the question of whether German regulation and law could apply in addition to that of Ireland remained unresolved. However, but this case's ruling on Article 4(1)(a) now indicates that German national law and regulation should apply. This jurisdiction of the CJEU will have a great impact on the law enforcement by national data protection authorities in the EU.
- It is important that major internet companies do not 'shop around' within the EU for the best location of headquarters based on the supervisory responsibility of the national data protection agency, as it would lead to a 'race to the bottom'.
- It is important that the proposed Regulation adopts a robust "opt-in" definition of consent.

BRENDAN VAN ALSENOY

- Alongside the question of prescriptive and adjudicative jurisdiction dealt with by Johannes Caspar, another jurisdictional question relates to the geographical scope of the implementation.

- How far should implementation of delisting stretch? Should delisting only effect local search results, or are there valid arguments for a wider, perhaps even global implementation? Google's current domain-based approach is local, which does not offer much effective protection in practice. The Article 29 Working Party has said it should apply to all relevant domains, including .com, but this approach has been criticised for imposing EU values on non-EU countries
- Google says 95% of its users that are directed to the national domain site will stay there. However, that statistic does not take into consideration the type of searches made (e.g. name versus other searches).
- Both sides of the debate have valid points and can learn from each other.
- Under public international law, territoriality is the primary basis for jurisdiction; however, in addition, the effects doctrine says that if there is a substantial effect within a state's territory, it may regulate. It is this same principle that underlies the application of article 4(1)(a) in Google Spain.
- The question of how to define how an activity affects another state has led to the introduction of the concept of reasonableness, and further, interest-balancing.
- Proposes four criteria (drawn up with Marieke Koekkoek) that could help determine whether or not boundaries are being overstepped from the perspective of public international law.
- The first criteria is the risk of adverse impact on foreign states, the second is the purpose of delisting (i.e. the underlying policy objective), the third relates to who you consider your attacker to be (e.g. nosy neighbour versus prospective employer) and the fourth relates to the territorial nexi of the original speaker.
- Google has convinced the European Commission in competition cases that domain-approach is sufficient to give effect. However, competition with its focus on ensuring fairness in the market has different thresholds than data protection which is to protect a fundamental right.
- As regards delisting requests under EU data protection law, a bid for global delisting may be justified in many instances but not all. In cases where the person requesting delisting is a figure of international interest (e.g., Max Mosley), delisting should be confined to "local" search results.

CHRISTIAN WIESE SVANBERG

- There are many reasons why the Regulation is taking a long time. The last Directive took five years to negotiate with only twelve Member States, now there are twenty-eight. There are also many commercial, political, societal and technological interests involved, not least those related to Snowden.
- The Council has a political incentive to pass the Regulation within the year; so although not everything has been agreed, the Council is moving forward.
- There is substantial agreement between the Commission, Council and Parliament as regards questions of territorial scope.
- There will be a large degree of extraterritoriality – the rules will apply to third countries. This will add work to the national DPAs and will create unrealistic expectations.
- Data processors are now to be directly regulated by the law which adds complexity.

CONFERENCE PROCEEDINGS

SESSION 1: THE PATHWAY TO GOOGLE SPAIN

CHAIR: DR. KIRSTY HUGHES, UNIVERSITY OF CAMBRIDGE

Both the breadth and depth of the Google Spain[1] judgment came as a surprise to many within the internet community. And yet, far from emerging in the vacuum, it built upon both general concepts in European data protection and particular concerns around free-text retrieval systems of public domain data which date back to the early 1980s. Moreover, since the early 2000s, the Court of Justice of the European Union has been building up a corpus of EU data protection jurisprudence increasingly based on the idea of data protection as a fundamental right overlapping with, but also distinct from, a traditional right to privacy. This reality was also strongly apparent in the Court's recent case striking down the Data Retention Directive. The first panel explored this background and context.

PROFESSOR ARTEMI RALLO LOMBARTE

Jaume I University and former Director of Spanish Data Protection Authority

Thank you very much to those organizing this conference for inviting me to participate here. It is a great pleasure, and I don't know if you're aware, all of you, but Professor Erdos is a visionary. He has one of the best qualities for academics because three years ago, he organized a very successful conference focused on the right to be forgotten.[2] And three years ago, it was not so clear that this will be a so famous or successful topic - the right to be forgotten and how the European court would resolve the topic then. I have to declare that he is really a visionary.

He has asked me to talk about the origin of the case, and I will try to do my best. Before 2007, there were not so many cases in the Spanish Agency related to the Internet - no significant cases. The story of the right to be forgotten, it started in 2007, with a first case. Related—because this is the beginning of our history — related especially to personal information in the official gazettes. A man in the eighties, a young man, was fined by the local police for urinating in a public street. The police were not able to notify this administrative sanction in the postal address, and the Spanish law established that it's possible to notify, in these cases, by publishing this resolution in an official gazette.

The notification was published in an official gazette thirty five years ago. All these papers at this time, who no one read at this time, were digitized. Currently, in 2007, this man—a professor, director of a high school — could check like all his students every first September through the Internet. And he found that thirty years ago, when he was young, he was urinating in the public street. This is a funny case, maybe, for it's possible some of you have a smile for this case, but I'm sure that for this data subject it was not so funny a case.

He complained and he reached a positive resolution. The Spanish Agency ordered Google to erase links and avoid future access. Official gazette where at the beginning the problem, because it is obliged to publish many personal information. For example – pardons. The pardon law in Spain, is obliged to publish the government resolution of pardon. In this case, like many others, the man was pardoned, the pardon decree was published in the official

[1] The judgment can be found at: http://curia.europa.eu/juris/liste.jsf?num=C-131/12

[2] Materials from this conference can be found at http://www.csls.ox.ac.uk/conferences/oxpilsconference2012/index.php

gazette. At the beginning, thirty years ago or twenty years ago no one read this kind of information, the news this official gazette had written. No one was interested. But all of them were digitized. And as seen in this case and many others, they found that everyone with access to the Internet could read about this information.

Professor Artemi Rallo Lombarte, 27 March 2015, University of Cambridge

The Spanish Agency ordered Google to take the necessary measures to remove the results of the index and to avoid future access. And to the official gazette, the Spanish agency obliged to take the necessary measure—not to delete because there is a law which obliges them to publish this information - but to take the necessary measures to avoid future indexing. That means to use tools like the robots txt.

We could talk very much about the official gazettes; for example, other laws established that civil servants' sanctions, disciplinary sanctions, must be published in the official gazette. In this case, a person – civil servant – was sanctioned and the resolution was published in the official gazette. What happened, at this time in the nineties, [was that] prison civil servants were [the] target of terrorist attacks by ETA (the terrorist band). In this case, the Spanish Agency, accepted this complaint. Later came cases related to newspaper. But none current online newspaper [but] especially news related to old, written newspaper that were digitized. And that paper, from thirty/forty years ago, now everyone can read them, in this case or many others that happened. For example, this one, La Vanguardia, main Spanish Catalan newspaper, published, in 1989, news related to a man who killed his son pressing a pillow against his face, sleeping, in October [19]87. He was acquitted for this crime in the trial because the court considered paranoid schizophrenia. But the newspaper never published anything about that. Thirty years later, every time he accessed the Internet, he found this information, and that affected his illness. In this case, like all the others related to the newspaper, once more the Spanish Agency urged Google to take these measures to remove data from the index, avoid future access, but related to the newspaper these digitized news, the Spanish Agency considered that not only there is a law, even there is a constitutional right - the right of freedom of speech - that prevailed. And that means that the Spanish agency has never obliged to remove or to erase archives from the

newspaper. What the Spanish agency said to the newspaper, in these cases, is a recommendation to consider individual circumstances to avoid the indexing by the search engines. That means using tools like robot.txt.

We could talk about very much cases related to newspapers, not only old news like this one: [19]91, a crime, someone is on news on the El Pais, main newspaper. There is news informing about a crime—a plastic surgeon who finally was acquitted. But never the newspaper informed about this acquittal. There are many cases [which] maybe we could talk later about. But I will finish this landscape about these cases with the one that was launched to the European Court of Justice, with this preliminary ruling. The case of the European Court judgment. A strange case. The national Spanish court could have chosen any other—it has 150 cases to choose. It chose just this one. Once more La Vanguardia published information, not news, just public information. A public body, from the Social Security, obliged or ordered the newspaper to publish an administrative resolution related to an action on real estate caused by a freezing order derived from debts to the social security. That means that this was not news of public interest more than after this first dissemination, but not for the future.

I'm sure you are questioning yourself about the grounds of the Spanish Agency to adopt this position. For me, I think it is very easy to summarize these grounds because all of them have been accepted—mainly all them—have been accepted by the European Court of Justice. All of them can be found inside the European Court of Justice. That means that the Spanish Agency, like the European Court judgment, establish that the European law was applicable—is applicable—to the search engines with advertising office in a member state, that the search engines process data, are [a] controller, have direct responsibility, independent of the webmasters, and that it is possible to react against this personal information using the right to object or the right to erase. That there are limits, of course, freedom of speech and information related to public persons or news of public interest – this is the limit. All of this has been established in the judgment and was in the Spanish resolutions.

Especially, the main ground of the Spanish agency was better explained maybe in the European Court of Justice. That means that for the European Court of Justice and for Spain, the search engines are not [the] subject of fundamental rights. That means they have legitimation for processing information but this legitimation just is an economic interest. They have an economic interest; they are not [the] subject of freedom of speech. They are not media. And that means that in the conflict between data protection and the search engines' activity, legitimated by the economic interest, the first one prevails. This is in the core of the European court judgment and it was in the core of the Spanish resolutions. Differences: just one. The European court goes further than the Spanish agency, who always resolved case by case, taking into account individual, personal circumstances in any case. That means more or less accepting just the right to object more than the right to erase. The European Court judgment had said no: the right to object is a tool, is a way, but the right to erase too. And why? Because [it] has well explained that the passage of time changed the meaning of the information—the passage of time affected to the quality principal, because information becomes inaccurate, excessive, inappropriate, or obsolete.

> *Victory of the judgment has many owners; but I have to share with you that the Spanish resolutions, that the Spanish agency had not allies in this struggle -any allies. That is the truth.*

I will use my last five minutes sharing some additional thoughts. Victory of the judgment has many owners; but I have to share with you that the Spanish resolutions, that the Spanish agency had not allies in this struggle—any allies. That is the truth. That means that internet users were not allies. When I say internet users, I am relating to the evangelists of the net, of the web, of the internet - activists [and] organizations who think that the internet is a way for freedom of speech. Of course there were allies - maybe the data subjects, the victims this dissemination of information, who complained to the agency. DPAs, data protection authorities, and especially the Article 29 Working

Party were not allies. National DPAs, all the DPAs around Europe, were in different way and in fact, Article 29 in its opinion in 2008 on search engines last used three lines, in a footnote, talking about special national legislations for relating to the Spanish case. They were not allies. Some national judges, it's true, that react in the same way, not the Spanish judges which launch into the European court, a preliminary ruling. And mass media were not allies. I have to make a difference: mass media affected by these resolutions, never accepted in the first years this kind of resolution. They didn't apply the Spanish Agency resolutions, but it's true that they broadly disseminated the topic. It has a big impact like information — the right to be forgotten.

That has changed. I can share with you that for example, last year, El Pais, main Spanish newspaper, adopted a new style book. In this new style book, it specifically states that it recognizes the right to be forgotten. That means accept[ing] explicitly delisting news, old news, more than fifteen years old news, never news related to sexual abuse judgments nor accepting erasure of archives of course and accepting notice for updating news. This is the way in which the Spanish Agency has many times recommended newspapers to react. And of course Google was not an ally. It always appealed all the Spanish resolutions and in which way with grounds. It is easy to find these grounds. You have just to go to the opinion of the Advocate General in 2013 to find all of them and even more—the Advocate General was the best lawyer Google could find. It is true that the Advocate General accepted that the European law was applicable to the search engines and that they process data—they were controller- but he makes the difference between responsibility of the webmasters and not responsibility for the search engines. The problem was how it considered the right to be forgotten. For the Advocate General the main difference with the European Court judgement [was] the right to be forgotten. The intention of someone to delete personal information, who never authorized to be published was just a subjective preference—this is the word, a subjective preference. He doesn't consider it like a human right, a fundamental right, even he said a terrible expression that that Article 8 of the Charter of Fundamental Rights just repeats what the Directive 95[/46] established, and make a big difference with the European Court, which really founded all its judgment on the consideration that the right to be forgotten considered like this is inside of the right of the personal information right considered like a fundamental right like Article 8 of the Charter established.

And one second, or one minute, just one second to tell, that I think this judgment in this case, which started with other judgments of the European court, is in some ways a new and significant political jurisprudence, started with the case Snowden and with other, many other cases related to it, data retention cases and others.

JEF AUSLOOS

KU Leuven

So let me start by thanking David and Julia for inviting me here today. As a matter of fact, two years ago I was here as well talking about the exact same case at the time that the hearing had just taken place, and it's great to see that at least from an academic's perspective (maybe not from an industry perspective) that it's there's still so much attention to all these issues.

So earlier this month some of you might have seen this big live-streamed debate in New York between Paul Nemitz, Jonathan Zittrain, and two others. So I was very surprised at the time that even between these people, but also in many other debates, that there's still people mixing up different issues, different concepts, different rights. They're not talking about the same stuff, actually. Still so much misunderstandings are injected into the debate, which often makes, you know, not for a constructive debate. So that's why I thought that I'd take this opportunity at the beginning of the day also to, you know, clarify and delineate some of the issues so we are all on the same wavelength for the rest of the day. Of course there's many things I could talk about, so I tried to centre them around two main topics. So first of all, the conceptual issues and secondly, the whole censorship argument that often always comes back.

Mr Jeff Ausloos, 27 March 2015, University of Cambridge

So first of all, conceptual. So, as you all know, the right to be forgotten is a very evocative concept, void of any clear legal meaning, but we are all kind of guilty of using it in this debate. So I'm sure most of you know the movie this picture is from. *[Indicates to the presentation.]* The Men in Black – they have this device called the Neuralyzer, which makes witnesses to an alien incident forget what they have just seen. And so, in debates often this right to be forgotten is considered to be the legal equivalent of such a Neuralyzer, which frankly is a bit absurd; we cannot make people forget what they have just seen, let alone with a legal instrument. So, if you look more closely at this term, I think it makes more sense to look at it as an umbrella term for a lot of already existing rights. The *droit à l'oubli*, or [the] right to oblivion if you will, the right to object, the right to erasure, now the right to be delisted. So I'll quickly run through them.

Droit à l'oubli, as you might have guessed, French origin. It's case law-based; there's no clear legal ground. Depending on the facts of the case, judges have used the general right to privacy, IP rights, tort law even — so it all depends. The underlying rationale is actually to prevent [the] republication of information that would have a disproportionate impact on an individual. The classic example is the ex-convict, who ten years after being released from prison, sees information popping up again. So it's this whole idea of starting anew, with a clean slate. By definition there will always be a conflict with information freedoms, but if you look at case law, courts have always found a balance and there is only a limited number of cases this right has been accorded. And traditional media outlets have also developed code of conducts, you know, to deal with these kinds of requests. And of course, with the digitization of news archives, and the Internet in general, the potential number of cases has increased dramatically in the last decade or two.

So right to erasure and right to object, contrary to this *droit à l'oubli*, right to oblivion, they have a specific legal ground in the Data Protection Directive. And so rather than focusing on avoiding publication of information, these are intended to empower data subjects in the relationship with data controllers—to exercise some control over

what happens with your data and to that extent you could look at them as sort of tools in the data protection tool box, that could be used for a variety of purposes.

And then, finally, the right to be delisted originated in the *Google Spain* case, though it was never explicitly used as such by the Court of Justice itself. It's only in the aftermath that people start using it, but now it's commonly accepted as the term to refer to use in this context, even by the Article 29 Working Party. In here, the rationale at least at the court's side and it's because search engines create such detailed profiles of information on whatever you're looking for, combining information from all over the Internet—combining and compiling a very detailed profile. And of course this is the main reason why we use search engines in the first place, but it also explains why it has such a potentially big impact on whatever you're looking for, especially if that's a person.

And in a way, this is a great example of where all of the previous rights overlap, right? To a certain extent, the goal is similar to the *droit à l'oubli*: avoid further publication. But specifically based on data protection rights, targeting a very particular processing operation, and because I cannot stress this enough and you still see this misunderstanding in debates: it's a very narrow scope of application — it's really about the link between a name search, between a search term and a search result. I'm certain I will talk about this later during the day — to what extent this might translate to other kinds of search engines — internal search engines, website-specific search engines, or other information intermediaries like social networks for example.

Okay, the censorship issue. Unsurprisingly, the ruling was welcomed with a lot of, you know, with a massive panic attack about how it would be the end of freedom of expression online. And indeed, many find it very surprising that the Court did not mention once this fundamental right to freedom of expression. So what I will try to do in the last five to ten minutes of my presentation is say: don't panic. I'll do this by going into four different kinds of arguments that we often see returning.

First of all, public versus private nature of personal data. This is often presented as a binary: even if information, personal information, is published in the tiniest corner of the Internet, it's part of the public domain and there would be no limits to its further dissemination, you can freely link to it, et cetera, et cetera. In this line of reasoning, soon everything will become public, right? Because so much stuff is being digitized today and with your smartphones, all of our interactions happen online. Bruce Schneier has called it 'the loss of the ephemeral'—everything is being stored today. And this whole line of argumentation, in my opinion, ignores that this public versus private nature of data is not a binary — it's actually a continuum, right? You have many different in-between states. Just to list a couple of them, there's depending on the case — you shouldn't look at it as one or the other. And depending you know, on the nature of the information or the nature of the publisher, the nature of the information, will you know, be on a different place on this continuum. It's all the idea also of practical obscurity that Woodrow Hartzog has written about.

So secondly, the position of Internet search engines. As you all know we're becoming increasingly dependent on search engines or any information intermediary for that matter to access all kinds of information online. Google is often the first page we go to when browsing the web, when looking for something. In that regard you could consider search engines as a funnel or strainer through which we access most information online. And this is, as I said before, their most valuable characteristic. To find the information you need, compile a profile as detailed as possible about your search term, with all the information that is out there. Now that's also the reason why it has such a potentially big impact on the person you're looking for, if you're using person's name as a search term. It's important to keep in mind that you know, that this funnel in the middle there, is the underlying decision-making process for compiling this profile on the basis of whatever search term is entirely or largely secret. It's by no means neutral. So we have to be aware, briefly, you know, that these are corporate black boxes almost unilaterally deciding what we get to see, and sure, they do a very good job of it, but we have to be aware that, you know, it's based on algorithms that are designed with a specific purpose in mind.

> *Actually so much of the arguments that you see returning in the discussions is that Google or search engines equal the Internet — and by extension, all information out there. If something would be removed from Google, even just on the basis of a name search, you would alter history. [W]e should be very wary of…considering them our window to the Internet.*

Alright, next. And this is related to the previous points. Actually so much of the arguments that you see returning in the discussions is that Google or search engines equal the Internet — and by extension, all information out there. If something would be removed from Google, even just on the basis of a name search, you would alter history. One of these Google hearings, I'm not sure where — I think someone from Index on Censorship even said that the ruling would endanger investigative journalism. So I'd be very wary of the investigative journalist who would only use Google as his primary resource. So they might be looked at as the strainer through we access information, so we should be very wary of them, of considering them our window to the Internet.

Paul Bernal, I think is here. In a blog post he argued that maybe we should look at search engines as we already look at Wikipedia: you know, it's a good start if you're looking for information about a certain topic, but by no means the definitive authoritative source. On that note, it's also interesting to see that Wikipedia has very strong guidelines in place enforced massively on the presence or deleting or maintaining personal data on their pages, so it also makes it very strange that Jimmy Wales was so heavily opposed in these Google hearings.

Alright, finally, the rights of publishers: often returning point, not touched upon really by the Court of Justice, what about the publishers? Don't they have a right? So first of all, I think this is a largely overplayed point — looking at the limited numbers that are available in Google's transparency report, we see that the top ten web sites that are targeted are by no means legitimate news sources; it's social networks, it's people's search engines, so all third parties actually by themselves. Do you really want to give these actors a voice? And, secondly and more importantly, I think this argument seems to presume that publishers have a right to be indexed in the first place. And of course - no one argues - that search engines play a very important role in exercising one's freedom of expression. You know, there's also a lot of European Court of Human Rights case law also protecting the means to effectively exercise one's right to freedom of expression, but does this imply that publishers have a right to be included in a search engine based on specific search terms? Should Google allow publishers to put their information in the top rankings? They actually do this already -it's called Google Ads. So we've got to get organic results; as I said before, it's a black box. Anyone even trying to game these algorithms risks what is the so-called Google death penalty — you know, being entirely banned from search engine. So this whole argument and the other arguments as well: aren't we giving Google too much credit? In a democratic, open society, don't we want diversity in our sources of information? In January this year, at CPDP in Brussels, Marc Rotenberg of Epic, he said that the news media suffers from a Stockholm Syndrome vis-à-vis Google. They're taken hostage by them but cannot live without. So I think I'll stop, and welcome any questions later on.

DR ORLA LYNSKEY

London School of Economics

Good morning. Thanks to Dr Erdos for inviting me and for organizing this conference, and it's a real pleasure to be back at Cambridge for the day.

I've been asked this morning to talk about the jurisprudence of the Court of Justice in the lead up to, or as a background to, the Google Spain case. There's been remarkably little case law in front of the Court of Justice dealing with data protection issues, despite the fact that we've had the Data Protection Directive for almost two decades. But rather than going case by case through the jurisprudence, which might be a little dry for the morning slot, what I've instead tried to do is to demonstrate that the case law prior to *Google Spain* is entirely consistent with the Court's findings in the *Google Spain* judgment. And I say this for three reasons. So I guess the subtext here is the reasons why we should have seen *Google Spain* coming, and I think that's for three reasons.

So first of all, the Court has continuously insisted upon the broad scope of application of the data protection rules. And that's something that is reflected in the *Google Spain* judgment, and you see that through, for instance, the broad scope of territorial application, which the Court gives to the Data Protection Directive in that case, where it says that Google search engine processing is in the context of the advertising activities of its Spanish subsidiary. So broad scope of territorial application there, something which the Advocate General was in agreement with. But then also you see this broad scope of application is affected in other ways, which I'll go on to talk about.

The second point, which I think is quite evident, is that, despite a slow start, the Court is now placing increasing emphasis on the EU Charter and in particular, on the EU Charter's rights to data protection and to privacy. So, unlike other international instruments, the EU Charter includes both a right to privacy in Article 7 and a right to data protection in Article 8. The Court has been quite forthcoming now in emphasizing the effectiveness of those rights.

And then the third point I think we could adduce in order to support the *Google Spain* finding, for good or for bad, is that the Court at present seems to be quite emboldened. It has taken several judgments, which illustrate in my opinion that it is not entirely concerned about the political fallout that will follow from its decisions. So I'll elaborate on these three points now.

So first of all, if we take the broad scope of application of the data protection rules, here I think you can see that the Directive has a broad personal scope in terms of how we define who is a data subject, and also as we saw in *Google Spain*, who is a data controller. So in that case, the Advocate General had argued that in order to be viewed as a data controller —so an entity, a company which would be responsible and or have obligations pursuant to the data protection rules — there should be a knowledge that the company concerned is processing as a company, could also be a local authority, the entity concerned. There should be a knowledge that there is processing of personal data. Now, a literal interpretation of the Directive doesn't include that knowledge criterion, and actually the Court rejected the idea that a data controller has to have knowledge that they are processing personal data in order to have obligations pursuant to the Directive. Google here might have been quite a particular case but I think if you look to the kind of broader issue the application of data protection rules that's actually quite sensible finding. Because in the absence of that finding, companies could plead ignorance of the fact that they are processing personal data in order to escape obligations pursuant to the data protection rules. But you see there that the Court is defensive of the broad personal application of the data protection rules.

You also see broad material scope of the rules. So here data processing is pretty much anything that you could do with personal data, and personal data is any information relating to an identified or identifiable person. Jeff has just spoken about identifiability and the issue of public and private in the context of things like anonymization, but I think it's important to highlight here that that definition of personal data goes beyond the type of data that might be covered by the Article 8 ECHR right to privacy. It's a very broad definition.

So we have this very broad scope of application of the data protection rules, and as I just said, unlike the right to privacy in certain contexts, this will always apply to material in the public domain. This is irrespective of whether the information is publicly available or not. This broad scope of application has been defended by the Court, in its case law. So it's very protective of the Directive's scope of application. So I've just indicated a couple of cases here

but in a case like *Schwartz*,[3] what was concerned with was the fingerprinting data of a German national who was obliged to provide this fingerprint data in order to obtain a passport from his local authority, in, well, through the German government at home, and he objected to this on the grounds that it was unnecessary data processing. The Court recognized without hesitation that this type of data, which would also benefit from the right to privacy, constitutes personal data in the context of the Directive.

Dr Orla Lynskey, 27 March 2015, University of Cambridge

A more complicated case, you might say, is *Bavarian Lager*.[4] And there you had a query about access to minutes of a meeting between industry representatives and European Commission officials. The Commission was refusing to grant access to the minutes of this meeting on the grounds that the names of the industry representatives constituted personal data. Between the Court of First Instance at the time, the Advocate General and the Court of Justice—there was a dispute about whether or not those industry representative names could benefit from the right to privacy because although there's right to privacy in the workplace, here it doesn't seem to sit very well with the reasonable expectation of privacy, given that the access was sought under transparency regulations at the EU level and equally, with the rationale for privacy in the workplace, which is to allow individuals to develop relations. And clearly, the whole aim of transparency legislation is to prevent cosy relationships between Commissioner officials

[3] The judgment can be found at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=143189&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=284366

[4] The judgment can be found at: http://curia.europa.eu/juris/liste.jsf;jsessionid=9ea7d0f130dea640e090a9b24d4babc4d054e3a4214a.e34KaxiLc3eQc40LaxqMbN4ObxuNe0?num=C-28/08&language=en

and industry representatives. So this might not have been covered by the right to privacy but it clearly fell within scope of the right to data protection, and of data protection legislation. So you can see again a broad scope.

Then, I think the most recent notable case on this is a case from last December, where the Court was asked to consider whether or not the exception to the scope of the data protection rules, which is an exception for personal data which are processed for purely personal or household purposes, could be applied to the case of Mr. Rynes.[5] Mr. Rynes was an individual who had installed a form of closed-circuit TV outside of his front door because his family home had been subject to numerous attacks in the past. So this camera was installed for personal security purposes, and it captured the pathway up to his front door but it also captured part of the public path outside of his front door. This camera happened to capture some footage relating to an attack on his house. The footage was brought forward to be used in the proceedings against the perpetrators, and the question was raised as to whether or not that footage could be used because Mr. Rynes hadn't received prior authorization for the processing, and hadn't complied with his obligations as a data controller. So was the capture of this footage compatible with data protection law? He argued that the processing in this instance was for purely personal or household reasons. The footage wasn't automatically recorded over itself; it wasn't retained. He didn't have a way to examine the footage remotely on a phone or anything else. And yet the Court found that that, in this instance, the footage was not purely personal because it captured a public pavement. So you see there, that that is a remarkably narrow interpretation of the purely household and personal processing exception in order to preserve the broad scope of application of the rules.

But in that case, the Court kind of was at pains to emphasize that just because you fall within the scope of the data protection rules doesn't mean that the processing is unlawful; rather, at that point, once you're within the fold of the rules, there is a system of checks and balances which determines whether or not the processing can be lawful in that particular circumstance. So you have a very strong indication from the Court there that Mr. Rynes would have been able to justify this processing, and that it would have been adequate.

So we have the broad scope of application, which is reflected in *Google Spain*. We also have an increased emphasis on the effectiveness of the EU Charter rights. So, I would argue that in the early years, prior to the Charter acquiring binding force or becoming a justiciable instrument in 2009, there was an initial reluctance on the Court to point to the Charter right to privacy in order to justify its actions in any given case. I think this kind of narrow interpretation of the Directive is particularly visible in a case like *Satamedia*[6]. So in that case you an issue about whether or not data on high earners — so those who were earning over 100,000 Euro a year — could be disseminated via text message by a private company. There, the private company had pleaded that this dissemination could benefit from the Directive's exemption for processing for journalistic purposes. So the argument was the text message dissemination is journalistic, and therefore can fall outside the scope of the data protection rules. And there the Court interpreted that journalistic purposes exception really broadly, so it said that it applies to the disclosure of information, ideas, or opinions to the public.

Fast forward to last year and you can see that clearly the definition of journalistic purposes has changed significantly when it comes to the *Google Spain* case. So we have seen, I believe, a change in a change in tack when it comes to what could benefit from this exemption for journalistic purposes.

[5] The judgment can be found at: http://curia.europa.eu/juris/document/document.jsf?docid=160561&doclang=EN

[6] The judgment can be found at: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-73/07

> *[T]here's perhaps in the Court's case-law, an indifference to the disconnect between law [and]…technological developments…*

Finally, I think in addition to that change in tack, there's perhaps in the Court's case-law, an indifference to the disconnect between law [and] it's maybe a bit harsh to call it reality, but certainly technological developments, and that, you know is one of the big criticisms of the *Google Spain* case. That's also a criticism of the *Lindqvist* case where the Court seemed to have kind of mixed feelings about how the Directive should apply to the Internet. So on the one hand it held that the act of a pensioner who was uploading data to a charitable web site for personal purposes, as part of her data processing course, could be criminally prosecuted for that action because it was personal data processing, because she uploaded information on her colleagues to the Internet. But on the other hand it stopped short of saying that she should have been responsible for international data transfers. So you can see that the Courts have kind of struggled to apply this old Directive to new circumstances.

Finally, I think you see, at the moment, a stronger Court, particularly when it comes to fundamental rights. This is perhaps because of, as I said, the introduction of the Charter, the Charter's acquisition of binding force in 2009. But that was very visible in last year's judgment in *Digital Rights Ireland*.[7] The Court, for the first time, struck down an entire piece of legislation on the basis that it was not compatible with the EU Charter rights. In so doing, it ignored the Advocate General's request that that the judgment have a temporal limitation, which would allow Member States to put in place arrangements for data retention while a new Directive would be enacted. So it ignored that.

But equally, I think if you look at something like *Opinion 2/2013*[8], which is where the Court was asked to assess the illegality of the European Union's accession agreement to the ECHR, with EU law. It found that that accession agreement to the ECHR was incompatible with EU law. In an incredibly kind of complicated judgment - which I think could be narrowly read - it effectively said that by signing up to the ECHR as the agreement stands, it would be circumventing things like the preliminary reference procedure before the Court. So again, clearly a case where it wasn't too concerned about the political implications of its findings.

Then finally, this week before the Court of Justice, we had the hearing in the *Schrems* case,[9] which was a preliminary reference from the Irish High Court, where the compatibility of the Safe Harbor Principles — so, allowing data transfers between the EU and the US — was challenged on the basis that those principles, which were adopted in the year 2000, no longer reflected a situation where adequate protection was being offered to EU citizens when their data are transferred to the US, as a result of the Snowden revelations. There, I believe, from everything I've read and heard about the proceedings, they were quite lively, and that the Commission was left more or less (I think I can say this) on the back foot, in arguing that in order to effectively protect fundamental rights, individuals should possibly not sign up to Facebook.

---

[7] This judgment can be found at: http://curia.europa.eu/juris/documents.jsf?num=C-293/12

[8] This opinion can be found at:
http://curia.europa.eu/juris/document/document.jsf?docid=160882&doclang=EN

[9] Documentation on this case can be found at:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=157862&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=328696

So, what it remains to be seen, and what will happen with that judgment—the opinion of the Advocate General is due on the 24th of June—but I would say, based on what we've seen so far, the ingredients would indicate that Schrems has a good chance of succeeding in that case.

FLOOR DISCUSSION, QUESTIONS AND RESPONSES

Question: A delegate commented on the emboldened nature of the CJEU asking whether it was a positive development. The delegate further asked whether the approach in Rynes was a positive development, extending data protection from institutions to individuals, and whether there were enough safeguards at the Member State level. He asked whether, looking ahead to Google Glass or drones, such an approach still made sense.

Dr Lynskey answered that whether the decision was a positive one or not was tricky to answer. The decision brings many individuals within the scope of the data protection rules although she could see the logic of the Court as otherwise much information would become incontestable from a data protection perspective even if an individual objected to it. It may be good for advocates of a risk-based approach as if processing is within scope of the rules there is an incredibly strong case that they should be subject to obligations that are far less stringent. If you apply the risk-based approach not as one of whether the rules apply or not but as one in which the scale of the obligations corresponds to the risk of the processing then you might say that individuals should still fall within the scope of the rules but would not be subject to many of the day to day compliance obligations that a regular data controller would. If there was particularly objectionable data processing you would not be left without a cause of action under data protection rules if you were an individual acting against an individual.

Question. A delegate asked whether you saw emboldened courts not just in the EU but elsewhere, for example in the US. The delegate asked whether it was a trend we are seeing around the world.

Dr Lynskey answered, noting that she was primarily an observer of the CJEU, that in the Irish courts there was certainly an increased recognition that data protection and privacy are, thanks to Snowdon, on the agenda. If you look at the reference from the Irish High Court, Justice Hogan states on several occasions that it would be naïve to not to think this type of mass surveillance and privacy invasion was occurring but nevertheless there was a need to refer questions. There is an increased awareness. She did not know what the courts in the US will do with this. There were also others better placed to comment on Vidal-Hall. It was perhaps becoming unsustainable for the UK not to allow damages from distress given the consensus in favour of this in other EU Member States.

Question: A delegate asked why the Spanish Data Protection Authority was able to hold that La Vanguardia was able to publish information on Costeja because even if it was legally justified at the time it seemed that they also should no longer be able to make that publicly available in the same way now. He asked whether Professor Lombarte could explain how they got to that position.

Professor Lombarte answered that the Spanish Data Protection Authority had taken particular care concerning newspaper activity to avoid opening the box of strong criticism focussing on censorship and to avoid erasing or affecting news archives. Most of the time the Spanish Data Protection Authority insisted on recommendations to avoid indexing from search engines. This was the main philosophy, recognising that the information was the same as in the publication.

Mr Ausloos asked whether it was also because the national data protection authority feels uncomfortable about the consequences of the decision, invaliding the law requiring publication.

Professor Lombarte answered that the national legal requirement did not go so far as to require publication in a paper but merely to ensure dissemination before the relevant auction. They were not obliged to publish in a newspaper, merely to disseminate the information.

Question: A delegate asked the panel what it felt were the reasons behind the emboldening of the court. The courts seemed to have become more emboldened over time. Leaving aside privacy and data protection, it is not so clear that the courts are emboldened in other areas, especially in the context of austerity. There have been a series of conservative rulings on social policy. He asked why privacy received special attention.

Dr Lynskey described her hunch that the Charter's reference to both data protection and privacy played a role. This was possibly an area where the EU could claim some sort of regulatory supremacy. Data protection regimes around the world are modelled on EU law. The Court is possibly quite protective of data protection and privacy. Such developments were backed up by the Snowden revelations and a trend towards EU/US divergence on freedom of speech, data protection and privacy.

Question: A delegate asked the panel whether information should be treated the same by data protection law if it became outdated or whether there were legitimate reasons for information to exist in a newspaper archive.

Mr Ausloos made a distinction between archives and search indexes. He questioned whether Google was the appointed archive of the internet. In the context of broader big data, policy discussions were needed.

Professor Lombarte answered that it was a difficult political question about freedom of speech. If an authority ordered the erasure of archives there would be a complaint focussed on censorship. Complainants were largely concerned about the indexing not erasure from the archive or online website. Their concern was just Google and the broad dissemination of the information via Google. What the data subject asked for and needs is just to resolve the problem of delisting.

Dr Lynskey considered that there was a legitimate distinction and there should be more limited grounds to remove from an archive assessed on a case-by-case basis.

SESSION 2: THE CHANGING LANDSCAPE FOR SEARCH ENGINES AFTER GOOGLE SPAIN

CHAIR: DR RICHARD DANBURY, UNIVERSITY OF CAMBRIDGE

The Google Spain judgment directly concerned the responsibilities of search engines vis-à-vis processing of public content, most notably through the actualization of a right to erase personal results in certain circumstances. This panel explored the developments to date, and potential future trajectories, of these now confirmed data protection rights and obligations.

WILLEM DEBEUCKELAERE

President, Belgium Data Protection Authority

Thank you Mr Chair, and I certainly want also to thank David for this fantastic opportunity, this setting here in this auditorium. I will come back to that because for me it's a sort of an ideal place to exchange ideas on this issue, and I think that it is very important to talk about this landmark decision which had enormous influence on data protection and on the work of the European Data Protection Authorities. I only have twenty minutes so it will be difficult to really go into all the details of this six-point presentation, so I will skip a lot of them. I will skip certainly some of the ideas from the cornerstone document that is the Guidelines. In November of last year the Working Party 29 adopted guidelines on how they understand, how they are reading, and how they are interpreting the case, the *Google Spain* ruling, and also giving thirteen guidelines how to work with the specific cases that will be asked.

It would be witness to an improbable Ivory Tower mindset to only invest in the protection of privacy or in a pure judicial approach. The issue imagined from the *Google* case is not only about the right to be forgotten, about applicable law - very important - about jurisdiction, but also on decision-making power – power in general.

> *Law is always a reflection of the balance of power.*

Law is always a reflection of the balance of power. Since Machiavelli, Hobbes, we are very aware of this. But in the twentieth century, we have accepted by trial and error, that a broad general human rights approach is possible. I know, I know "it's the economy stupid" - but if you want to resolve the issue in a democratic perspective, we have to realize that human rights have brought an important. That's why in this great building of the rule of law, there has been provided an additional floor, a solid roof, a shield that wants and has to protect the citizens from attacks against their freedom and integrity. So dear listeners, you will immediately understand that I won't limit myself to a judicial analysis. I think that if we are looking through the looking glass of *Google Spain*, we have also been impressed by the importance of the Charter of Fundamental Rights of the European Union of 12 December 2007. The judgments make the clear distinction between fundamental rights on the one hand, human rights, and interests in economic interests, of interests of the public. It's in the section 99, the four last sections, that it is really very clearly stated by the Court. And it's amazingly remarkable that not much attention is paid to this issue in the comments that recently has been written on the judgment just after the pronunciation. You could almost become cynical about it. I have read and heard different arguments such as "you Europeans have missed the point", "the internet doesn't work that way", "the ICT world has and imposes its own rules", "it's the technology", and as a final quote "that is not how our business model works."

Why is it so difficult to accept the ruling of the Court? Maybe because privacy or data protection has not been considered as a human right, but only as an interest? Should interests, rights in general, not be treated on the same level? There this one major exception: freedom of speech, free collection of information. I would be unfair to countless commentators if I wouldn't take this into consideration in my analysis. But even here I strongly would like to point out the clear and detailed assessment made by the Court of Justice in the ruling. There were lots of checks and balances that were carefully expressed. The task of a Data Protection Commissioner is embedded in the protection of the whole human rights [and] fundamental rights, and need to find the correct and safe balance between the different basic rights such as personality rights, privacy, protection of personal data, freedom of speech, free gathering of information, the right to the integrity of a person, security, freedom of trade, right of property, education, the house of the rule of law provides a lot of rules, countless floors. And if it can be sometimes difficult to find your way, this is one of the reasons why we today are gathering here in this conference. This auditorium should be a perfect power-free space. In Germany they talk about *Herrschenfrei* of Jürgen Habermas, where we can practice the art of the veil of ignorance.

So that was an introduction, now back to business. We tried, as Working Party 29, to find already in 2008 solutions for the questions [which] arise by the upcoming search engines. And we have this first document of 2008 and Artemi has already mentioned it. I don't think that today it is useful to read it, so I skip and turn to the next one.

What was the reception of the Court ruling? First thing, we were relieved because - can you imagine that the court should say, "well, European law is not applicable". In that moment, I think a lot of data protection authorities can close their doors. There was also a surprise. The surprise was that the Court clearly stated that the right to be forgotten is a fundamental right, is something that should be applied on the level of a human right. And it was a surprise because the Advocate General had not accepted this point of view.

There was also a lot of uncomfortable feelings – "how will we manage it?", because we thought thousands, tens of thousands, of applications would come to us. And also, will this sentence not have an inverse effect. Will the reaction, because it was certainly in the first weeks there was a very hostile reaction of a lot of comments. Should it not have the effect that yes, that legislators, that law-making will try to avoid the principles of this ruling? And lastly, I think

that there was also a very important boost into the world of the data protection authorities. We considered ourselves empowered because not only data protection can be empowered by the maintenance of law and order, but also because the Court has given us real practical tools to do our job protecting the citizens. We try to implement this ruling. There were exchange between different data protection authorities. We have also had a lot of meetings with people from Google - Peter Fleischer was practically every week in another capital in Europe. It was good to talk about it and we tried to seek a common position from all the twenty-eight countries. We made them make these guidelines, working out all the experiences that in the different countries we were confronted with. And then we adopted on the 26th of November these guidelines on the implementation. The structure of this document is one interpretation of the judgment - very interesting to read how we were also struggling with a lot of concepts in it - and secondly, trying to be effective, making a list of common criteria for the handling of complaints. Important do say to you, these are guidelines. In the letter that the document was sent to Google it was also clearly stated by Isabelle Falque-Pierrotin, the chairwoman the Working Party, that these are guidelines that can be reviewed, can be made better, in the course of time.

What is very interesting also is the first two pages of these guidelines because you have an executive summary; an executive summary that gives you a very short but very sharp introduction to the concepts that we find as Working Party 29 in the ruling *Google Spain.* Thirty nine of these are mentioned, and if you look to them you will see that a lot of these questions will arise also in the second, the third and the fourth panel today.

The criteria are of course the most the important of these guidelines, and then we have thirteen, I will not say that that they are really in a scientific way, criteria that you can use, but it also sometimes are more questions – questions that should help to resolve very practical situations where not only Google - because its Google in the first time who has to look to the applications - but then after appeal to the Data Protection Authority, they have to consider where we remove the URL, were we delink, and where indexation. Sometimes a question is divided because there are a lot of sub-questions. For example is the data relevant and not excessive. Of course that is not an easy question to answer.

Sometimes you have questions that are not completely in line with the ruling - for example the question of prejudice. It's clear that the Court has said you don't need to prove a prejudice, you don't have to demonstrate that for having the right to remove your data. After that we had issued these guidelines, we have tried in the Working Party to find also more substantial solutions for questions that were answered but in a way that not everybody was happy with, and I think there are still a lot of questions. But the most important, I think, is the question of the territorial validity and the enforcement. You can say "oh, it's only for the country involved", but that's not true. It's a European law so it should be implemented in the whole of Europe, which is what Google accepted. But maybe it is worldwide? Why is it worldwide? Well it is a personal right, and once a judicial decision has been taken about a personal right, it should be worldwide accepted. There is another question which is what do you do with a country without establishment, but that is really a question for the specialists. Another problem is a problem of more political weight is the Barbara Streisand effect: the more you are crying to be delisted, the more you are exposing yourself. A little criticism of Google: in the first weeks and months they were not speaking of the *Google Spain* case, but of the *Costeja* ruling. I tried to change that and to say let's talk about Super Mario, because it is Mario Gonzales Costeja, so I think we have to use the normal general denomination which is *Google Spain* and the rest. But there you see that this is also a question of power, who had the power to give a name to a certain sentence. There is also sometimes a problem of inaccurate data. I will not go into the details, but that is sometimes a very difficult thing to do.

But what is the reality? The reality and now I take this example from Belgium. We started with this one case, and ended yesterday with thirty-four complaints. Thirty four complaints – that is practically nothing. If you take into consideration that according to the numbers that Google has given, forty five per cent were not accepted from these items of request. So that means that only 1 cases out of 210 cases are coming to data protection authorities. We handled already twenty-one of them, sixteen have been accepted by Google, six were accepted by the Data Protection Authority, and only one is a question where we could not reach an agreement. The biggest problem for us in the beginning was censorship. We did not want to have this censorship. But in all the thirty four cases we have had, we have never had a problem with on censorship. And I will give you one little example. This is an extract of a

letter of Google where they denied to delete an index. The only thing they are saying is that the person in question was somebody who is a dangerous person, and, then, in that moment they say that we should be aware of the fact that he can in future relations also be dangerous. But I think we have also a solution for that. Google has accepted that if there is a court ruling to find a solution that he gets a clear criminal record that they should remove also this URL.

Willem Debeuckelaere, 27 March 2015, University of Cambridge

So I will come to my conclusion. I think that the question of this example is once again giving an example that the right to be forgotten, and also the questions that are arising by the *Google* case, will after all end here in judicial debate, but also in court rooms. And once again, today we are in a court room, because I understand also today in the High Court in Great Britain there is a sentence according to a problem arising from the use of Google search engines. And I think that I will again invoke the power-free space as requested by John Stuart Mill, Rawls, Hannah Arendt, and especially by Jürgen Habermas, because I think it is important to take that into account also in this auditorium. And such a sphere happened also yesterday in the premises of the CNIL in Paris where several data protection officials from European met a delegation of Google to discuss the terms and conditions that were put in place two years ago, and that were subject to several rulings of several data protection authorities. And that now Google has accepted to review them, and to give new terms and conditions I think in the month of June, that is, it will be this year. That is a very positive evolution, I think. That Google accepted the *Google Spain* sentence, that they comply fully and that they set up a system to implement this sentence.

And what we all should learn from this case is: one, that the data protection authorities must be brave and courageous like the Spanish, that we should be brave and courageous to impose instructions and decisions. Secondly, that human rights really exist. Not because they have been proclaimed, but by the fact that we are using them in litigation in courts. And third, at least, it is a question of power. And that in a democratic and a decent society this power is laid down in the law, executed by those who are bound by the law, and enforced by courts of justice.

WILLIAM MALCOLM

Senior Privacy Counsel, Google

Thank you Mr Debeuckelaere for those remarks, thank you Mr Chair, and thank you to David and Julia and Cambridge for bringing together this great group of people to discuss and debate what I think will continue to be some critical issues over the next few years. The speakers on the first panel expertly set out and clearly set the background to the case and all the issues, so I'm, in the interest of brevity, not going to touch on that. I intend to talk about Google's response and to give some insight into my practical experience and Google's practical experience in implementing the judgement.

Right from the start, right from this landmark ruling, Google made it clear that, although we didn't exactly welcome the judgement, we respected it. And it was our job to make it work. I'm very proud of the hard work that our teams have put in over the last ten months to give effect to the individual rights that the Court confirmed in this judgment.

As of 23rd of March, and as is publicly available in our Transparency Report, which I will talk more about in a minute, Google had received 843,000 individual delisting requests with respect to URLs, representing nearly 232,000 individual requests. Roughly speaking, we delist in 41 per cent of cases, and decline to delist in 59 per cent of cases. We publish a full Transparency Report at Google.com/transparencyreport where you can see these statistics which are regularly updated in terms of the volumes of requests we're seeing, and what are our removal rates look like. There is also a national breakdown, so you can see what those statistics and percentages look like at a country level.

So that's a lot of volume of stuff, and I think it's fair to say that's a lot of work. To individually assess 843,000 URLs takes a bit of doing, and, you know, we move very quickly to comply. We were very quick to launch a web form, setting up a process to manage these requests. We were very quick to engage with data protection authorities to hear what they had to say on the subject. And we listened to a wide spectrum of views through the advisory council process that we established.

Now let me say that our approach has been largely consistent with the recommendations of European experts and regulators, but there are still areas of disagreement. Some of which I will touch on when I talk today. Conflict of laws and jurisdictions are never easy, since fundamental rights are at stake, and fundamental rights are weighed differently in different countries and different parts of the world. But we are committed to listening to the debates across Europe as this issue evolves.

So moving on to our experiences of the last ten months. The first thing that we did after we read the judgement was to stand back and say, okay we need to have a way of receiving these requests. We were conscious that we needed the right amount of data to do the job. We didn't want to create an open channel where basically individuals would supply more information than was relevant for our purposes in assessing their request. And so we thought to ensure that we were only collecting the right data from individuals, we would launch a web form. And we put a great deal of thought into the design of that web form and how it was structured. I will call out the main pieces of information we ask for when someone wants to file a delisting request. We ask for the name used for search, more about that later, we ask for the contact email address. We also ask for an explanation for each URL, again more on that later. And then we also basically then remove all name query searches, so that was very clear from the Court's judgement, that the ruling was limited to name query searches, so not removing links for any or all search result pages, which could be overbroad, and this is clearly not required by the ruling.

William Malcolm, 27 March 2015, University of Cambridge

We focused on EU users. Our web form makes it clear that individuals need to select a relevant country. Practically, individuals will need some connection to that country, which will normally but not always mean that they have to be resident in it. Individuals need to select a country so that we know which law to apply, because there are divergences of practice with national authorities, as I will come on to in a minute. So it is clear which DPA the complaints should be remitted to. That's a practical problem, and our solution is the web form.

We focused on EU domains. We currently remove in EU plus EFTA states. We noticed early on that some data protection authorities called for pan-EEA consistency, and we wanted to support that effort. The most logical legal interpretation of this Opinion is actually for national removals, but for Google we thought it was right to take a pan-EU approach to encourage consistency and harmonization for individuals. When we remove a search result related to an individual's name, it will simultaneously be removed from all European versions of Google search. We do not remove on services targeted to non-European countries, including our US service on .com. When individual search on .com we already redirect them to the local relevant domain. In practice the vast, vast majority of our users use these local domains.

We do not think the Court's ruling is global in reach. It's an application of European law that applies to search services offered to European consumers. We have a long established way of complying with country-specific laws by removing from the version of our service that targets that country. For example, Google.de in Germany. This is how we have always processed national law removals for national law claims, like hate speech, to use one example, and defamation, to use another. The services on those domains are tailored for users in those countries in a number of ways. It's not just about legal compliance. They are intended to be the best experience for the user in that country overall.

> *[W]e felt very deeply that we needed to be transparent about both the results and about the process that Google*

Another key aspect of Google's implementation of this judgement - we felt very deeply that we needed to be transparent about both the results, and about the process that Google was running. So we have a generic notice at the bottom of our search results that when a user enters a name query search for most names about a person, that information will be displayed. And now let me be clear that the notice that fires on the bottom of our search results page is not a notice that is fired with respect to any specific removal. It is a notice that is fired with respect to most name query searches. And we think it's important to give our users information about the results that they are seeing, and how those results have been compiled.

Also, we think it's important to notify webmasters. This is consistent with the approach in other removals. We are giving webmasters the link or URL that will no longer appear in search results as a response to a query research, not any details of the request. We have long done this in other areas of law, not just for removals made on data protection grounds. We have also let people know on the web forms so that they are aware that this will happen. We believe it's important to let third party publishers know when we stop linking to their sites in response to some queries. And we have already started seeing complaints from webmasters about the prospect of removing links to their sites, and we are already facing challenges from publishers about removal decisions that result in reduced traffic to their sites.

We provide this feedback to ensure transparency and address those criticisms directly. We have received communications from webmasters that has caused us to re-evaluate removals and reinstate them, and in some situations third party publishers may want to publish the underlying content. With the right to be forgotten, of course, we as Google, the data controller with respect to search, have a legal obligation to assess each case. However, and sometimes, you know, users may get the perception that filling out a form on Google removes it from the original source. And so actually notifying webmasters may alert the original source to the user's position with respect to the material in a way that actually produces a practical result for the individual. In others, webmasters can identify whether an accusation takes traffic away from their site, or was mistaken, or was inaccurate.

Next I want to turn to this issue of what kind of information we have when we make the decision. Clearly, there is this large carve-out for public interest and we had to decide how to apply that. When we assess a request we have the information from the web form, and we have the material from the site. We do not have any information from the publisher or speaker. And we think it is important to ensure balance in the process that we have that opportunity. There is of course no journalistic exemptions for search engines. That was made clear by the ruling. But at the moment there is no established way for a publisher or speaker to feed back or to be aware that a particular name query search has been delisted.

We will continue to give careful thought to these issues, but we believe we are taking the right approach. However, we recognise that there is a spectrum of strongly held views on these issues across Europe within the privacy community, and even differing views among European data protection authorities. As we continue to discuss these issues with data protection authorities and others, as we evolve our processes, we will, you know, continue to keep an open door and an open mind as to what comes next. For example, we recently introduced a policy not to send webmaster notifications to certain categories of sites, such as malicious porn sites as I have noted previously.

As most of you know, the criteria laid down by the CJEU were fairly vague. We worked hard to develop criteria to apply to the myriad of real world situations, some of which I am going to talk about, which we faced when dealing with the requests that came before us. It was a broad ruling with little guidance on application. Our challenge was to evolve our approach. We accept that our policies and practices will change over time based on what we hear from

data protection authorities and what we hear from courts. In that respect, we welcome the guidance of the Article 29 Working Party. We were comforted by the fact that much of the removal criteria was similar to the removal criteria that we had already developed and were implementing. And actually, that consistency between the approach we were taking, and the recommendations of the Working Party was comforting for me and others at Google.

I want to turn a little bit to the guidelines and some of the ways that Google thinks about the issues internally, and some of the trends that we're seeing. We want to be thoughtful and pragmatic about where we decline to delist. A big area is public figures where we have a general expectation that we will do fewer removals. So I'll give you a couple of examples of cases where we refused to remove. A footballer who wanted to remove a news article about his career highlights, a TV star who wanted us to remove news articles about a recent sex scandal. There can also be a figure in the public eye because of what they do in their professional life. We have had removal requests covering a respected scientist who wanted to remove criticism of his scientific work. And, you know, there are challenges here. But even public figures, you know, basically, when you're looking at these news stories, you have to take into account that they have a public personae and a private personae. And some of the calls are difficult, and we are seeking to develop more nuanced criteria as we move forward.

Another area of contention is news stories. When someone is mentioned as a meaningful part of a news story, again that's a real indicator for us that that might be something that we would decline to delist. If the source is a reputable news story, if we are dealing with a recent article, then, you know, clearly, generally having access to this information we feel is in the public interest.

So there are challenges around that. Another area of challenges is political speech, and to give you some examples of areas where we have pushed back. Members of the government requesting the removal of news articles about their corruption scandal, police officers involved and being convicted of bribery and corruption or having disciplinary charges in relation to bribery and corruption levied against them. Pushing back on a request from a member of government requesting the removal of posts of citizens criticising policies. So these are real examples. And there are really, really difficult examples in political speech. We get a lot from people who want to clean up their past at university. They say I was involved in a political society at university, and, you know, I'm no longer active in public life and I want to remove or delist all name query search information in relation to the statements I made at that time. In some cases they say that when they are in fact running for political office. And in some cases they say that when, you know, you know, when clearly what they are doing is trying to limit the field of information that is available online. So these are challenges and where we draw the line on these is something that we will continue to evaluate.

I want to move on to some trends, then, and some issues we are seeing. Complete volumes to data protection authorities from what we can see at this point are relatively low in relation to the 840-odd thousand URLs we've received removal requests for. Very low. I put them in the hundreds. I see every one of them personally, and I put them in the hundreds. But let me try and draw out some of the things we are seeing. We got some data protection authorities who are ordering us to remove government records, simply on the basis that the government site is the right place to find that government record, and that there is no public interest in linking from a search engine in response to a name query search. We've got some complex cases involving defamation where it is not clear to us or the data protection authority whether the content in question is true or not, but we are nonetheless being ordered to remove. And again I welcome and call out the Article 29 Working Party's guidance on defamation in that respect. As one might expect, the criteria on past crimes and when it is appropriate to remove a past crime diverge significantly nationally, even if one has common criteria. There are individual rules across Europe and in various countries with respect to the treatment of past crimes and so we are seeing difference in standards there in the way that the data protection authorities are approaching the issue.

Recency is an issue. We often get asked, well, how many years for this and how many years for that. And we have to say we have to judge each individual case in all of its merits. So our approach is much more dynamic than that. We look at a range of factors and we don't draw hard lines, because that would be inappropriate. And we also have, as

I mentioned before, sensitive issues and political content, and these issues tend to cause difficulties. We've got one case at the moment where we are asked to remove a re-reported case, so that something that had been removed and then a newspaper has reported on the fact that there was a removal. And we've got one request from a data protection authority to remove that re-reported case. So you know, some trends are starting to emerge for sure.

I would also like to call out the work of our advisory council. We welcome all their advice and guidance, and we are considering carefully how to implement that. I would also like to point out that advisory council members do not adjudicate on individual cases. I think there has been some public misunderstanding about that.

So to close, our response will not be static. We know it will change over time and we know that data protection authorities will have guidance for us. We plan to learn from experience. We remain committed to engaging in thoughtful collaboration with the Working Party and with individual data protection authorities to discuss these issues further. In parallel, across Europe, national courts are starting to build a body of jurisprudence to interpret and apply the CJEU decision. Over time, collectively, we are gaining experience in processing removals and developing a better understanding of the implications of the judgement. We know that DPA's views will differ from our own in some cases just as the DPAs would reach different decisions amongst themselves in some cases. But we will only push a case if there is a public interest in clarifying the position. We know that tough debates lie ahead, such as on scope of removal and the right of publishers in the process. We think it is important to have those debates openly, and respectfully. Our door is open, we're listening and we want to work with those in the room and data protection authorities as we move forward.

We know that tough debates lie ahead, such as on scope of removal and the right of publishers in the process. We think it is important to have those debates openly, and respectfully. Our door is open, we're listening and we want to work with those in the room and data protection authorities as we move forward.

JULIA POWLES

University of Cambridge

It takes a rare legal case to capture the public imagination, and an even rarer one to stay there. I want to talk about why *Google Spain*, particularly in the context of search, is such a case. Why it is so fascinating, miserable, and inexhaustible as a source of debate from boardrooms to dinner tables. This requires us to roam somewhat out of the usual terrain of lawyers. This case raises questions most importantly of power, particularly, informational

This case raises questions most importantly of power, particularly, informational power. It's about promises, particularly the law's promises. And it's about privacy, particularly about privacy in a surveillance-based economy.

power. It's about promises, particularly the law's promises. And it's about privacy, particularly about privacy in a surveillance-based economy.

Before I get to those deep, subterranean issues, I've been told I can be a bit provocative so I'm going to take the opportunity and react a bit to some of what we heard this morning and in the last few, probably much more diplomatic presentations. I have two outstanding challenges or concerns that I think date right back to when this case was decided. The first, and this might sound a bit shocking, is that we don't really know what we are talking about. Sure, we might know about the law, about institutions, about balances between rights and interests. But what we don't know is anything more than a vague notion of the problem we are trying to solve.

At last count, 234,000 people had made requests to Google under the right to be delisted procedure. Their concerns range across the full spectrum of human experience. And yet Google has spoken publicly about only thirty one cases. Now we've had, I just counted, another four from William. But we have no indication of the relative frequency of these examples, any sort of greater representation of which balances they involve, how complicated they are, and so on. We have heard that the great majority of these requests are in fact a straight delisting – yes or no. But in the cases that are complex, do we need extra layers of information and intervention? I would argue that this isn't just about extra detail or embellishment; it goes to the core of what we are trying to deal with. The paucity of information prevents us from actually developing robust, useful, enduring, and considered solutions. It exacerbates misunderstandings and it promotes ideological and intercultural conflict. It means that we, the citizens, are faced with appeals from a variety of actors who all have their own vested interests, whether it is from private companies, from regulators, from politicians and the media; all of whom are saying: "trust us". There is evolution in the system. But I would say it is still unsatisfactory.

When I have spoken to people at search engines, I'm told that the detail can't be exposed because of privacy concerns. "We don't want to talk about individual cases", they say. But I'm not asking to be told for example, that somebody stabbed their ex-girlfriend eight years ago and now cannot have a relationship anymore, or to ask about somebody's medical results and the particular details that have been put on Google's index. It is to know whether two percent or twenty per cent of these delisting requests involve criminal cases, the sort of examples that William was talking about. It is to know whether , in relation to the large number of requests to Facebook, are these people who are delisting results on their own name, on posts that they themselves have done, and for which they are not utilizing the opportunity within Facebook itself to take down posts? Or are they things another person has posted, or indeed on some of the more despicable sites that you have on Facebook, are they from people they don't know?

What proportion of these requests concern mainstream media? The entire public debate has been about mainstream media outlets. But in the UK, the mainstream publications, the BBC, the Guardian, the Telegraph have all had in the order of thirty to sixty delistings. That's a tiny proportion of 234,000 requests. So I think that we end up generalizing from the particular if we don't have a greater understanding of the contours of the landscape.

Now in saying this, it is not that I want to criticize what Google is doing. It's to improve the processes, and so ensure that the law and the principles that we have are adapted to the problems we are actually trying to solve. I think that here the DPAs have an important role to play in leadership – Willem talked about that they have thirty four cases in the Belgian DPA. There are about two hundred in the ICO. We should have the cases de-identified, and reveal some greater information. We shouldn't bury information about how those cases are being dealt with. I think we have a right to know how they are being dealt with.

The other reason why I don't buy the search engine defence that this is about not revealing private information is because if that concern was real we wouldn't have the notifications to webmasters. From the webmasters I have spoken to at media publications, it is trivial to re-identify from a notice who has made a request, because you can have a one-click search at the bottom of a Google search result on a European page, and it flips over to Google.com, so you can identify immediately by putting in the URL, and the names in the articles, who it's about.

Julia Powles, 27 March 2015, University of Cambridge

The second outstanding issue, if that's what we're talking about, is who is talking. Every indication I've seen suggests that the bulk of these requests are about people with no public profile. They are victims of algorithmic failure. They are about normal people, and they don't have a platform to redress speech with more speech.

By contrast, almost all of the people talking about the right to be forgotten, do come from such a platform. Polling suggests that most people don't have information they want delisted online, but those that do, really do. And I'm concerned that those who speak out most about the right to be forgotten are not representative of those who really are at stake.

On that note, and this has been suggested on a number of occasions to me anecdotally, but I don't think anyone has said it in public, I think there is a huge unacknowledged gender issue too in who is speaking about the cases, and how the differential impacts of the rights of the right to be forgotten are felt. This is particularly the case in some of the examples that are brought up a lot in the media about revenge porn, for example, but I think I have yet to see a panel where there is anything more than a couple of women speaking, and I think that this affects how we discuss these issues in public.

So that is who is or who is not talking, and what we are and what we are not talking about. But let me get to why it matters. I said it is about power, promises and privacy. I think the *Google Spain* case is an externality of at least three much deeper issues. The first is about the vast informational power of search engines, and particularly *the* search engine, over so-called truth, memory, and history. As distinct from the comparatively disenfranchised individuals, who create, are the subjects of and consume indexed content. The second issue, since I'm not going just critique the private companies, is about the fundamental tension between the aspirations of European data protection law, and the capabilities and expectations of ordinary internet users. And the third issue is what we might call the surveillance-industrial complex of the twenty first century.

The force and hostility of many of the loudest reactions to the prospect of modifying search results on the basis of data protection requests, shows the extent to which we have comprehensively and largely unwittingly come to rely on privately-owned culturally biased black box services in navigating digital space. We have outsourced, the raw material, design and execution of multi-layered search strategies in return for easy, efficient interfaces and mysterious algorithms. They are of course wonderful, and deservedly Google has benefitted from network and economic effects, gaining an extraordinarily dominant market share, particularly in Europe. But this has created asymmetries of power.

For Google, completeness and trust are essential virtues of search, and this is why the case is so significant, and why it has amassed extraordinary resources in responding to it. By highlighting one way in which search results become incomplete, and I'd say it's by far not the most significant way, as privacy requests are outnumbered one thousand to one by copyright requests, and there we see nowhere near the same level of public debate.

But by highlighting one way that search index is incomplete, it brings the issue of consumer trust in Google to the forefront, and it has knock-one consequences for its financiers, the advertisers. From the beginning, it has been identified by Google's founders that search engines driven by advertising are "inherently biased towards advertisers and away from the need of consumers". This merchantability concern we have to keep at the heart of our consideration of the issues, because it explains the enthusiasm for analogies like "Google is a library card catalogue", happily we haven't heard any of them today, and that it is "a curator of history, truth and memory."

And of course this implies a pure and mutual collation service, rather than one that operates dynamic statistics-based search services over indexes that are only partially complete, and of course fall short of the much vaster, richer canvas of social history, truth and memory. So I think in all of this there is an opportunity for consumers and regulators to see search engines and other privatized engines of public space as, not catalogues, but also as dealers that can be optimized and gamed.

We also have to confront an impossible conflict that has been maintained to date by intermediaries, which is when accused of bias, they are exercising scientific opinion, and when they are asked to address privacy, they are merely neutral intermediaries. I think that this is a real opportunity, and we have seen a very willing approach to try to redress that imbalance. But so far, particularly on that copyright/privacy concern, we see that economic interests have driven what intermediaries have done, rather than human interests or personal interests.

The nub of the problem is that internet companies have been successful in making us believe that the internet is public space, when it is just a representation of privately owned services. They are not public parks, they are not the Greek agora to build politics, and yet the notion of public space is critical to democratic community-oriented rule. If we concede that the internet is a public space, then do we want privatized engines, and Jeff touched on this, to be the custodian of our public records? Or do we want to have them to be accountable according to what we would traditionally have for public utilities? I think this issue is only just starting to be addressed in Europe as the sort of leader. It is also in the competition case that's ongoing in Brussels, and it's a question of how we deal with these private companies that are the core of our public information goods.

Since I have to move on, I will just say that this power dynamic flows into the second issue, which is the question of the disconnect between European data protection law and how people use the internet. Even if, as Artemi said, the Spaniards championed this case on their lonesome, and then the CJEU was emboldened, as Orla said, it has been the case that the entire debate has been quite narrowed by the rapid and somewhat idiosyncratic response of Google into the actual application of the decision. A lot of this has been validated by the regulators [in the Article 29 Working Party's November 2014 Guidelines], but we are dealing only with post-hoc notice about whether information should or should not be processed. There has been no discussion of the issue of sensitive data, which has under European data protection law a near blanket ban on processing by data controllers without consent. The issue has been constrained to name searches, when, in fact, if you give me three pieces of information - your address, your profession, and where you were, or an image - then it might be very easy to identify somebody. And the question of

the regional localization has been dealt with through the frame of what is Google's version of national localization, rather than anything that's IP address-based, or based on physical real location.

Continuing then with the second issue, the disconnect between data protection law and reality, I think that the general public has never really appreciated the staggering reach of European data protection law, and this is the first time for many that they are grappling with it. The system we have, it's been promoted, and is politically at the moment being championed as a real solution to issues of privacy online, but I think it is woefully inadequate. The clear normative core of data protection is missing, and the reforms maintain some of those inadequacies. It may be, and some of the more heretical advocates in this area talk about the fact that we may need to have more public law style remedies or ombudsman-type remedies, rather than relying entirely on private processors and privacy agencies.

I don't have time to get into that anymore, but I think that the final point, the third aspect that I wanted to just say is that I do think this case, and the issues it embodies, are a step towards data sovereignty and freedom in an ever more connected reality where nearly every instance of our social and private lives is mediated by private companies. It's no exaggeration to say that this is about the struggle for freedom and control in a digital eco-system that is defined by surveillance. And it may be a fight in only a tiny corner of that eco-system, but it is important nonetheless.

I haven't made that connect too strong due to time, but I think that the connection between having real and meaningful rights against ownership of personal data in private search engines is an important essential first step. It is a litmus test of whether we could actually countenance these rights in any of our other interactions with digital media, which becomes ever more important as we have ubiquitous computing environments mediating every aspect of daily life.[10]

I do think this case, and the issues it embodies, are a step towards data sovereignty and freedom in an ever more connected reality where nearly every instance of our social and private lives is mediated by private companies.

EDUARDO USTARAN

Partner, Hogan Lovells

Good afternoon everybody. So this session is about the changing landscape for search engines. So let me lower the intellectual tone that you have put sky high, Julia, by making it simple. In very simple terms, search engines are now subject to take down requests as a result of or on the basis of the right of erasure. That's it. Okay? That is the changing landscape for search engines. And I think that is the main conclusion. Since I have a few more minutes to talk, I would like to explore a little bit some of the, perhaps, some of the finer points, going back to the decision, the Court of Justice decision. Some of those finer points that were made by the Court. Because, for example, the Court merely skimmed through critical concepts like personal data and processing. When you read the judgement there

[10] An extended form of this talk appears in J Powles, 'The case that won't be forgotten' (2015) 47 Loyola University of Chicago Law Journal.

are seven paragraphs, of about on average four lines each, covering personal data and processing. Which if you print it is about half a page. So there were assumptions of course that were made, but, for example in relation to personal data, the view that the Court took, was that the data that was being indexed by Google and by of course any other search engines in this case, qualified as information relating to an identified or identifiable individual, which of course is the definition of personal data in the Directive. But once the Working Party devoted a sort of forty page document to simply dissect that sentence of information related to an identified or identifiable natural person or individual, the Court just took that view that because this information does relate to people, and therefore that's being indexed, then that's personal data. The question is, is it personal data to the search engine? And that was not looked at.

Just looking at the definition of processing, of course what the Court said was that all this organising and again indexing, and making information available, that squarely fits with the definition of processing, because processing as we know covers pretty much anything you can ever do with data, digitally at least. And the Court went on to say that that was the case, despite the fact, or regardless of the fact, that search engines do not distinguish what they actually do with that information, they do not distinguish the nature of the information. They just do that technologically or algorithmically, or however you want to describe that, with all the information that crosses the internet. But that is processing of personal data.

And in line with this thinking, of course what the Court did, in a little more detail, was to expand, or to interpret, the concept of controller, which of course is defined in the Data Protection Directive. And I can see that personal data and processing can be absolute concepts. So it's either personal data or it isn't. It's either processing or it isn't. But controller, when you look at the definition in the Directive, is down to that subject, that entity, making decisions. There is an intention in being a controller. That's the whole point. It is determining the processes and the determination involves decision-making. My understanding of the word. But it is not an absolute concept. It is a concept that involves some thinking: "this is what we're going to do with the data." That's what the controller does. They do the thinking, they do the decision-making.

And the Court of course took the purposive interpretation of this definition to say, "ah but the objective," they used this word "the objective" of the definition in the Directive is precisely to make it really broad so that it covers any activity dealing with data. So when you add all this, of course, the interpretation of personal data, the interpretation of processing, the interpretation of controller, the implication, this changing landscape for changes, it is very clear cut. Not only are search engines not "intermediary" in the sense that and intermediary is someone that is not really responsible but somewhere in between. No, no, the search engines are the super-controllers. There is no controller in the world that I can think of that processes more personal data than a search engine. If you think about it. It is the biggest controller ever. Applying this criteria, it is the super-controller, and there is no one that processes more personal data therefore. I am not exaggerating. This has to be the implication, which means that all the obligations that apply to controllers will apply to a search engine. All the obligations, and then you look at all the principles, and the conditions for processing of personal data, and of course personal data we know has a sub category of sensitive personal data. So if you add that dimension to certain grounds of processing sensitive personal data, then you start thinking but this is just much more than the right to be forgotten, then.

But then you start thinking, hold on. No one has said, or maybe no one has been heard saying it at least, that the implications of this are such that basically this search engine model is simply non-compliant. And the reason why that's not being publically said, or at least by regulators I don't think have said it, is because it is seen as having gone a bit too far. And the reason why it is seen as having gone a bit too far is because it has an unintended consequence and here is what we see sometimes with a decision that can only be taken so far. Because if it is really taken all the way in terms of the implications it should really have technically speaking, it has unintended consequences. Is this a weakness? Is this a reality of life in an imperfect world? Maybe it's a bit of both. But this is an issue that is certainly raised by this decision. An imperfect decision for an imperfect world.

Eduardo Ustaran, 27 March 2015, University of Cambridge

But there seems to be great implications to all of this at least from a legal perspective, because it does not just affect search engines, it affects everybody else. It is the determination of the applicability of the law, which is also addressed by the case. And I mean this is what has really messed things up for everybody. Because the way in which the law, or the Directive, was interpreted in terms of the applicability of the law, we know when we look at the Directive, the criteria are relatively straightforward. We have Article 4(1)(a), applicability determined by the establishment of the country in the EU. 4(1)(c) applicability determined on the basis of where the equipment is located of course when the controller is elsewhere [i.e.] the controller outside the EU, but the equipment in the EU. Here we've seen a mixture of the two. It is, I don't know, 4(1)(c)(+), or however you want it. Because the interpretation that was given is: the controller is really outside the EU, everybody acknowledged that, but an establishment exists in the EU. And the kind of the link of the two is what determined the applicability of the law.

So this seems to have been accepted, but of course, regulators in Europe are now looking at this and are applying this local establishment criterion to situations where the controller is in the EU. Not necessarily in that country, but somewhere in the EU. Not outside the EU. No, in the EU, somewhere in the twenty-eight Member States. But the applicability of the law is being interpreted as EU-wide, so where until now, until very recently, we had the certainty that an EU-based data controller was only subject to the law of the country where he was established, now we are seeing the law being interpreted in such a way that an EU-based controller is subject to the law of that country where he is established, and everywhere else in the EU, wherever there is some form of presence. Even if the controller is not based there.

So to conclude I think that sometimes we talk about the European Commission being very ambitious in their policymaking. We're about a year away from seeing a law that is probably the most ambitious data protection law we will ever see in the world. We don't even need to wait for that. The Court of Justice of the European Union, in just one judgement, a twenty page judgement, has extended and created the greatest extension of European data protection law ever attempted. And that is why this case is so massive. And that is the changing landscape for search engines and for everyone else.

I think that sometimes we talk about the European Commission being very ambitious in their policymaking. We're about a year away from seeing a law that is probably the most ambitious data protection law we will ever see in the world. We don't even need to wait for that. The Court of Justice of the European Union, in just one judgment, a twenty-page judgment, has extended and created the greatest extension of European data protection law ever attempted. And that is why this case is so massive.

FLOOR DISCUSSION, QUESTIONS AND RESPONSES

Question: A delegate asked how representative the examples given in the Google Transparency Report were.

Mr Malcolm answered that Google would be updating its examples and statistics regularly.

Question: A delegate asked whether data protection authorities would be able to publish more information on disagreements between data protection authorities and Google.

Mr Debeuckelaere answered that although a decision had not been taken, the possibility needed to be looked at. There should be more statistics on the matters coming up. It was necessary for Google to publish information as well. It was not always easy to work with anonymised cases. It was also important for scholars that this information was available. It was important that they were made available with due respect for privacy.

Question: A delegate asked whether the problem for the Court in Google Spain was that it had only two choices: either Google was a data controller or it was not. If it was not then people with a complaint would have to go to California. That was the real problem. The delegate considered that the Court had decided it needed to protect individuals in Europe and therefore Google had to be a data controller so it interpreted data controller widely to achieve this. The court was given a hard choice and the decision to find Google was a data controller was a conclusion that flowed from the desire to protect individuals.

Mr Ustaran agreed that the CJEU was taking a policy making role. Knowing the outcome you want and then reasoning to it is the art of being a lawyer. The 1995 Directive as drafted is not really suited to this kind of issue and requires legal gymnastics. The Advocate General did not manage to do that. He disagreed on precisely this. The Court can decide whatever they want to decide. He did not think Google was a controller.

Mr Debeuckelaere added that the question of establishment was the important point. It provided the nexus for jurisdiction. The Directive was written when there were mainframes. The whole landscape had been exploded but

required working with the same concepts and rebuilding those concepts. Legal thinking must provide answers to the questions posed to it even when the law does not give a clear answer.

Question: A delegate noted that defamation is almost always present in the most serious violations involving inaccurate data. The delegate asked why the Working Party guidelines suggest that only trivial inaccurate data is the concern of data protection and defamatory matters should be referred elsewhere.

Mr Debeuckelaere agreed that data protection authorities should not send such complaints away. There was a fear of intruding on the competence of the police and criminal law but the data protection authority should not send the person away.

Mr Malcolm added that neither Google nor data protection authorities were able to adjudicate whether content is truthful. They are not necessarily in a position to adjudicate whether material is inaccurate or not. Further discussion was needed.

Question: A delegate asked whether Google was now in effect a super-regulator. Another delegate added that Google was quicker and more thorough than States are often when implementing decisions. The delegate asked for thoughts on what the Regulation should say about implementation.

Mr Malcolm answered that both Google and data protection authorities are committed to transparency. Google had published a lot of information quickly, statistics and examples, and were looking for ways to enhance it. It was committed to implementing the decision, although there were legitimate questions to ask about how to achieve the balance. This could be debated in the trilogue for the new Regulation.

Ms Powles added that there was merit in the German proposal for a triage process about complicated questions, a triage to a body that acts across search engines and which would take into account, for example, publisher interests. Delisting and maintaining links for name searches as binary alternatives is a blunt tool. There needs to be consideration of ways to link retractions to the original article.

SESSION 3: THE GENERAL SHAPE OF EU INTERNET REGULATION AFTER GOOGLE SPAIN

CHAIR: DR JUDITH TOWNEND, CENTRE FOR LAW AND INFORMATION POLICY, IALS

Background: Whilst the Google Spain judgment directly considered data protection vis-à-vis search engines, it is clear that its broad understanding of personal data, data controllers and data protection as a fundamental right have significant implications for the general ecosystem of the internet especially as regards data aggregators, online forums, rating websites and social networking sites. This session focused on exploring elements of this broader substantive context.

DR DAVID ERDOS

University of Cambridge

I'm going to make three claims about this judgment, which is ostensibly only about generalized search engines, and the internet ecosystem as a whole. In some ways, I'm following on from Orla's excellent presentation this morning in some of these claims. Hopefully there will also be some differences and a difference of emphasis as well.

So the first claim is that *Google Spain* in fact largely solidifies, or at least the fallout from Google Spain in terms of how to DPA's have responded to it, solidifies the dominant data protection paradigm. A paradigm which is dominant legally and even more so is dominant amongst data protection authorities. And that paradigm has serious implications, not just for the generalized search engines, but for almost every type of internet actor. You might say, "well how can that be?" in the sense that *Google Spain* was seen as so novel and so distinctive and in a way so narrowly cast on one particular actor. Well I think it's because there's a huge gap between legal

Enforcement has been extremely limited and sporadic. So extremely limited and sporadic that much of the Internet community until the Google Spain decision was virtually unaware any of these things in principle could apply.

interpretation, the interpretive stance including of data protection regulators, and enforcement. Enforcement has been extremely limited and sporadic. So extremely limited and sporadic that much of the Internet community until the *Google Spain* decision was virtually unaware any of these things in principle could apply.

So what is this paradigm I'm talking about? Well it's composed of four key pillars I think, some of which map onto Orla's various elucidations. The first pillar is that not much is excluded on the Internet from data protection and that has two elements to it. The key terms of the Directive have an extremely broad scope. We know this right back from the *Lindqvist*[11] case, where simply referring on an internet page to working conditions or hobbies of an identifiable person was processing of personal information. It didn't matter that it was an unstructured page. It didn't matter that the information was relatively trivial. Fast forward to *Satamedia* and the claim there was "oh but there must be some kind of public domain exception", at least if the material has already been published in the media, surely there is some kind of exemption for media published material. And the Court said: Absolutely not. Personal information is any information relating to an identifiable person. Processing is virtually anything you can do with data and regulated processing anything on the digital type device is always covered.

The second element of not much being excluded is that the exemptions are exhaustive and extremely limited. Again *Lindqvist* showed the way on this. It dealt with the scope of EU law being an exemption and the Court said: Well that's only about state authorities performing highly specific state-like functions like national security. Even that we now see much more debate about. Private and family life, they said, could never relate to indeterminate publication, could never relate to publication generally on the Internet.

Satamedia reiterated those precise claims and also dealt with the idea - "well aren't there some kind of implicit exemptions here?". No - the limitations on scope, they said, were exhaustive and they were narrow. That's the first pillar.

But you might say "well *Satamedia* said okay we don't have the exemptions but we have a special journalistic and other expressive purposes, so is there an issue?". Well, yes because the second pillar is that the special journalistic and other purposes are in no sense unbounded. They're not unbounded because even when they apply, as *Satamedia* said, any derogation has to be only as strictly necessary. We're not dealing with an exemption, we're dealing with a derogation but more importantly for our purposes they are not unbounded because despite the language of *Satamedia* saying disclosure to the public is a journalistic activity that public is a collective public. It's disclosure to the body politic. It's trying objectively to contribute to a general public debate. That kind of activity is included but that does not mean that any form of indeterminate publication, for individualized privatized purposes is covered. And again we kind of knew that from the *Lindqvist* case, where poor Mrs Lindqvist's website was clearly an indeterminate publication and the Commission sought to come to her rescue by saying: oh well her pages are a literary or artistic work - it's a work of literary and artistic expression and should be treated as such. And the court pointedly refused to accept that as valid. It didn't address it but it refused to say: yes of course this is expressive

[11] The judgment can be found at: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-101/01

purposes for the purposes of [the] special purposes. Mrs Lindqvist's site was not orientated to a collective public debate.

Dr David Erdos, 27 March 2015, University of Cambridge

But the third pillar is yes there might indeed be a need to balance data protection with other rights, and even with the general principle of proportionality, and we again know this from the *Lindqvist* case. Effectively what the Court said in *Lindqvist* was: we're not willing to say you're a journalist, we're not willing to say you're exempt but, by the way, authorities and courts must take care to ensure that the Directive isn't interpreted to be in conflict with freedom of expression and similar rights.

But it's rather unclear because another strand and the last pillar of the data protection paradigm is that data protection norms are often overriding. There is no particular need to balance with freedom of expression. Any need for balance has already been accommodated within the data protection regime and the key case here is *Bavarian Larger*, where you had a transparency request, the first instance court sought to say:Well we'll look to see if privacy and integrity are violated, we'll kind of eyeball it, we will not apply the rigors the data protection law if we don't think privacy and integrity are being affected very much. [But] the Court of Justice eventually said: No that's not what you should be doing. Any undermining of privacy and integrity must always examined and assessed in conformity with all the legislation on personal data. You simply apply the statute; you apply the code.

So that's the paradigm and it's shared by dominant legal interpretations but even more so it's shared as a dominant regulatory approach. If you ask DPAs, as I did, what they're interpretative stance is, you will find: very broad scope, a limited notion of what journalism and the like is, and then a dispute as to when you balance when you don't need to balance. And that broad contour applies broadly to all online operators from news archives - and by the way

there's an interesting debate about when the full rigours of the right to be forgotten apply because Google News as I understand it as an aggregator is considered to be fully within the right to be forgotten but maybe The Times newspaper index, for example, isn't but at what point do you move over from one to the other - it's a complicated issue I'd have thought - but anyway from news archives to bloggers to all forms social networking to dating web sites, street mapping, as well as search engines. Every internet actor is in principle affected by this paradigm.

I sought to test this empirically through a survey of European Economic Area - so EU plus the three associated states - Data Protection Authorities and got a very good response of eighty percent of the national data protection authorities replied, plus six operating at the sub-national level, mainly in Germany, so it's a pretty authoritative result. I presented them with publication scenarios linked to all of those seven online media actors which I've been talking about. This was before the *Google Spain* decision was handed down. And in terms of interpretative stance it backed up a very rigorous in principle interpretation of this paradigm. A maximum of only twelve percent of the standard answers as to these publication scenarios - which by the way are in your handout in terms of the very precise questions which were asked[12] - but they concerned everything from a blogger, news archive to a street mapping service. Across all the examples a maximum of twelve percent of the standard answers in any one case said that the activity was exempt from data protection. In terms of special expression, a plurality of Data Protection Authorities only considered that the journalistic or allied special purposes exemption applied as regards news archives - much to my surprise, even in the case of the individual blogger blogging about celebrity gossip there was not a plurality of support for the idea that the activity is journalistic or a like. Apart from the news archive and the blogger, where in the case for a blogger there would seem to be support for the idea you did need to have a balance with other fundamental rights, between just under fifty percent and almost a hundred percent of DPAs simply responded that data protection law had to apply in full. So, you know, really rigorous interpretation of the law in principle and not just for general search engines [but] for pretty much all internet actors.

So what about enforcement. I also asked for them: have you actually taken enforcement action in these areas, and if they had actually there was also an element of the questionnaire which I won't go into about what enforcement action they had taken. And I think the results here were intriguing in a way were the flip side of the broad interpretative approach which I've been talking about because this was the very narrow nature of enforcement. Almost twenty five percent data protection authorities said: oh we might have this broad interpretative approach but we've never taken any enforcement action since the Directive has been in place against any these actors in relation to publication. Then if you look at the next two [categories] along where roughly ten percent [each] have only taken action in one or two cases which might be, say for Google Street View. You are looking at a picture in terms of enforcement where almost a half of DPAs have effectively never really taken any significant enforcement action despite that being the paradigm and there I think use you begin to understand the dynamic where the Internet community seems to be unaware that data protection is considered to apply. Well, it's unaware because there's been so little enforcement of it. I asked about budgeting and the survey seemed to suggest that perhaps the average budget of a DPA is only around three and a half million Euro which translates into roughly €0.30 per individual resident in the jurisdiction. And I think you can see that that kind of level resourcing is just at a total mismatch at the level of tasks the law sets Data Protection Authorities because this is just one relatively discrete area that DPAs are meant to be regulating. This is by no means the only part that's meant to be regulated. It's got to regulate the public sector, it's got regulate all forms of data of which publication is just one and three and a half million Euro is simply not going to come anywhere near performing that task. And I also tried to complete, along with many research assistants, a public domain analysis of enforcement, which to be honest showed much less evidence of active enforcement. I mean what evidence there was showed very soft forms of enforcement and very limited forms of enforcement, compared to what was being reported in the survey. So even less seems to be [evident] - in terms of regular and active activity - than those results I just showed you a moment ago.

[12] A copy of this handout may found at the end of this Report.

So just a few brief conclusions and looking to the future in a way because obviously these conclusions are what I began with, but is there any real reason to think that this will change? I think it will only change if it is recognised that it is dysfunctional have a situation where the interpretative stance of regulators is at such variance with the practice in terms of how that is in reality enforced. It will only begin to change if we have a debate about the dysfunctionality and costs for the rights people think they have, for the responsibilities that controllers might have. If we start to have that debate about that balance and gap being a problem. And also it will only start to change if we begin to address the resources and budgeting that regulators have available in this area to perform what, in an Internet area, are more and more important tasks of balancing people's rights to be protected against freedom of expression.

DAVID SMITH

UK Deputy Information Commissioner

I suppose I should start by saying what a pleasure it is to be here but I have to say it's with some unease that I'm here. Particularly in front of those who study the work that we do as a regulator. I think I should sort of know what I'm doing but I think many of you probably know more about my job than I know about it myself. Actually, there is just a note perhaps of caution there in what we're talking about. Because some of you do analyze what we do as a regulator and you say "this follows this" and "there is this pattern there" which sometimes is true but very often we just, I hesitate to say we make it up as we go along, but we just do what is right at the time.

David has an uncanny ability to make me particularly uneasy because you say "well you said that in that piece of guidance two years ago and now you're saying that today" and "how does that tie-up with this judgment on *Satamedia* or whatever". And I think I ought better to answer it but I haven't got the foggiest idea. I'm not sure that they did. Not everything necessarily does tie up and I wonder, if certainly for us as a regulator, I wonder if even with the courts a little bit and the CJEU whether you can analyze it too far and sometimes they just decide what's right on the day and in the circumstances.

I have to say David you made me even more uneasy by inviting me very kindly to the post-conference dinner at Trinity Hall which I'm sure much to its regret declined to have me as one of its students some forty three years ago when I applied to them. But you didn't know that unless it's on Google of course! It probably will be now.

What I want to do now and I have not got long is to talk just a little bit about how we see the judgments as the regulator, put it in a wider context, and then talk about not just the Google judgment but about the forthcoming Regulation and the impact that will have on the shape of EU regulation and the Internet.

So the judgment, we've talked about this, the crucial thing really for us was that the Court decided that Google was data controller, the way in which it processes personal data. And the clear message that we read from that is "look, you don't escape EU law by some argument that you are neither a controller nor a processor or that you've come along since the legislation was developed and you are not caught by it. Eventually the law will catch up with you. So if you're doing anything as an organization or a business on the Internet that involves you manipulating information about individuals that has some sort of impact on them, you get caught" and – it's not "it's not personal data" or "we're not a controller" - you get caught. And of course you get caught territorially on applicability but I'll leave that for discussion in the next session.

And then of course, Chris Pounder I think was right, once you get to "you're a controller", EU law applies. Then it's just binary. Once you are a controller, the whole obligations of the Directive then fall on you to comply with. Yes - that leaves us with a bit of a mess. There's a quandary: things like sensitive personal data. Forgive me David, don't ask me to answer that. There's a problem there. But it will be solved somehow at some point and it's the right direction that we are heading in.

Of course implementation of the judgment - yes, there are critics of it - but there are 200,000 people now who have complaints to Google and nearly half of those have had the URLs removed and very few have ended up as complainants to Data Protection Authorities. So there are, I hesitate to say, a lot of satisfied people or a lot of people who have had real concerns and whose up privacy is better protected now so it is having exactly the right effect.

But let's just look at it in context. Again others, particularly Orla this morning, have talked about this as just part of the way the CJEU case law is going so I won't develop that further. I think what is very important for us is the emphasis that is being placed by the CJEU on the Charter and particularly on Article 8, the right to data protection and seeing that coming through and we, I think all of us in this data protection community, owe a huge vote of thanks to a former chair of the Article 29 Working Party Professor Rodota. I have to say, not for the way he chaired the meetings, but for the work he did in actually working politically to get this data protection right inserted in the Charter of Fundamental Rights which was being developed. I don't think any of us, other than him, realized how important it would be and it really is making a big difference now. I think we are seeing this - not necessarily the Charter itself - but the direction of travel flowing through into the UK courts.

David Smith, 27 March 2015, University of Cambridge

There was a case, just a High Court case,[13] a few weeks ago in Northern Ireland concerning Facebook where an individual brought a case to court against Facebook and against someone who was running a Facebook page on

[13] CG v Facebook Ireland Limited [2015] NIQB 11. The judgment can be found at: https://www.courtsni.gov.uk/en-GB/Judicial%20Decisions/PublishedByYear/Documents/2015/%5B2015%5D%20NIQB%2011/j_j_STE9491Final.htm

"keeping our kids safe from predators." This was about outing paedophiles who had served their sentences and who were being rehabilitated into the community.

The Court there, not under data protection although data protection issues were raised, fined, not just the person running this page but Facebook themselves 15,000 pounds, I think it was, on the basis that they had a responsibility for the content that other people will putting onto Facebook.

We just got this direction of travel where Facebook isn't just a neutral place where you post information and it's only sort of between the individuals who posted it and the people who see it.

I'm sure Hugh will tell us more about today's Court of Appeal judgment which is all part of the same trend.

We talked about the courts being emboldened. I think we as regulators are emboldened as well because we've got a fair wind behind us. It's all going in the right direction of travel.

I remember we at the ICO took a case up, this must be getting on for ten years ago, about police retention of data in the UK and essentially the police retain criminal conviction information forever and we thought that was excessive in data protection terms and although we won our case at the first stage tribunal, the Court of Appeal came down heavily against us. I think the Court of Appeal, well they might come to the same conclusion now, but their reasoning and approach would be much more favourable to our position now than it would have been. We've got, as I say, a fair wind behind us.

I think also, and this isn't the Google case, the Snowdon revelations do have a real impact on internet regulation in the future, the lack of trust, the impact on encryption - can we encrypt our messages and trust encryption? - the impact that this has on the draft European Regulation, where we see some of you will know Article 43a introduced by the Parliament, which attempts I think to do the impossible, to reconcile what's a conflict of laws. I mean, everybody points to the US but it's not just the US. Where businesses in Europe are required by US law to release information on, some significant penalty, from the US but releasing that information would actually be breach of the European legal framework. I have to say we as regulators can't really resolve that, only governments and international treaties can. But it's all playing into the proposed Regulation/the future Regulation. I think what we are seeing is that case law under the existing Directive is moving us actually closer to what's proposed in the Regulation, so maybe when we get the Regulation, eventually maybe a year's time from now, it won't be quite the leap that we were expecting because the case law will be a long way in that direction already.

Just a couple of points about the Regulation. I won't go into detail about all of these but the material scope - that processing of personal data is huge - everything is caught. At one time we were talking "are IP addresses is caught by this?". Clearly they are now as technology moves on and we move to IPV6 they will be even more clearly personal information. So again technology is taking us more towards IP addresses being personal data. The law is taking is more to it. It's all converging.

Territorial scope we will not cover.

People place a lot of emphasis on consent and as a regulator I get very concerned about those who see consent as the answer to every problem and if we just give individual's consent to everything, you know, they will be protected that will be fine. And in practice, of course that doesn't work. People don't make informed choices, they just plough ahead. We need to think more intelligently than just seeing our consent as the answer.

We have the "right to be forgotten" in the Regulation as it was called although whether that will be the title at the end [we'll see] because it was just as inaccurate as a title in the Regulation as it is about the *Costeja* decision. But what we do have there, that I think is very important, is this "right to object" where, put very simply, the way the law is currently structured, I can object to your processing of my data whether it's on the Internet or not. But I have to make the compelling case to you as to why that should happen. The onus if it goes through will be the other way around. I make my case, I just say I object, and you have to make the compelling case as to why you should continue

to process. And I think, although there's been very little attention, if that comes through and that right exists this it really will shift the balance of power and put some very important rights in the hands of individuals.

Just to talk about the exemptions and derogations. David would think I was amiss if I didn't talk about the exemptions for freedom of expression. What I would just say, these are hugely important and the whole basis of the Regulation is about harmonization across Europe, the same rules. Yet when we come to the exemptions for freedom of expression these are left up to Member States. I happen to think that's right because I think harmonization is a step too far - more consistency yes - maybe not harmonization. So we still will see I think potentially significant differences in how this is applied.

I know I've only got a minute or so left so just a word about our role as supervisory authorities. I don't make any pleas, but life is getting more and more difficult for us. The Google decision, these decisions on what should be taken down, what links should be removed, are very difficult decisions. I mean there are extremes - anybody can make those - but the ones around criminal convictions and if it should just be spent convictions that come down. And what if they are convictions to do with commercial businesses fraudulent trading and you're still trading? Even though it's a spent conviction, should that go? Some very difficult decisions.

I have to say I think the *Rynes* decision makes life even more difficult for us because it does take us into processing by individuals. Yes you have your CCTV camera on your house, it's overlooking a public area and I think must be, by extension, if it's overlooking a neighbour's garden, then that's probably not within the domestic exemption. So how do we deal with warring neighbours over someone's camera snooping on another? It's not just difficult to deal with the individuals who are complainants. Our tools, the enforcement tools we have, don't enable us to deal with that. We have monetary penalties/administrative fines but they are not there for individuals. So we will make it work. We have this arrangement - the one-stop-shop - the consistency mechanism coming up through the Regulation which as it goes through discussions, in particularly the Council in Brussels, is just getting more and more complex. There are pages and pages just about how we ensure consistency across Europe. So I just come back to the point to conclude with, that Orla made, about the courts suggesting they might be indifferent to the disconnect between law and reality. I worry a little bit the same about those who are now drafting the Regulation and, particularly as we get up to the trialogue process, is there going to be a disconnect between those who are trying to come up with a legal instrument that solves everybody's problems and brings the whole of Europe - all 28 countries - together in one solution. They may do that, but will it address the reality? I think one of the realities in the end has to be this access to justice. It's all about individuals and protecting individuals. Thirty pages of sort of legal niceties on how the one-stop-shop operates don't actually help individuals. They need simple, clear law - rights which are easy to exercise even if they're not perfect. And we aim a bit too much for perfection and not enough for effective rights in reality.

I think one of the realities in the end has to be this access to justice. It's all about individuals and protecting individuals. Thirty pages of sort of legal niceties on how the one-stop-shop operates don't actually help individuals. They need simple, clear law - rights which are easy to exercise even if they're not perfect. And we aim a bit too much for perfection and not enough for effective rights in reality.

HUGH TOMLINSON QC

Matrix Chambers

Good afternoon and thank you to David for inviting me to this extraordinary event. I see so much knowledge of data protection gathered in the room, probably about as big concentration as you can get in this country. It's a very welcome scenario to have so many people here to discuss these issues.

Jude raised at the beginning of this session the question of the broad impact of *Google Spain* and there's absolutely no doubt that *Google Spain* has an impact across all forms of Internet services. In a way that is at the moment completely unpredictable. And it doesn't work very clearly in practice. I mean I've just be asking a few people in the course of the day how it is that Google ever manages to process sensitive personal data lawfully. The answer is, it doesn't seem to be able to, but it seems to get away with it. Someone ultimately is going to try and work that through in the courts or the regulators.

[T]here's absolutely no doubt that Google Spain has an impact across all forms of Internet services. In a way that is at the moment completely unpredictable. And it doesn't work very clearly in practice. I mean I've just be asking a few people in the course of the day how it is that Google ever manages to process sensitive personal data lawfully. The answer is, it doesn't seem to be able to, but it seems to get away with it. Someone ultimately is going to try and work that through in the courts or the regulators.

I'm going to focus, in my presentation, on two very narrow issues from my experiences of litigating these issues in the English courts. I think that they are possibly of wider significance. I just want to deal with two aspects. The first is, it's been promised and I'll do it, is the case of *Vidal-Hall v Google*,[14] which judgment was handed down today by the Court of Appeal. For those of you who don't know what the case is about it's to do with something called the Safari workaround, by which Google was able to obtain browser generated information from users of Safari, either deliberately or accidentally. I think there's an issue about that. But obtaining information which they shouldn't have been obtaining. Effectively a class action has been brought in England and it's necessary to serve those proceedings on Google in California. That means under the English rules of procedure you have to get through certain gateways for service out of the jurisdiction and one of those gateways is to demonstrate that you have a claim for damages.

So there's a data protection claim and the barrier to a claim for damages is section 13 of the Data Protection Act because, as I'm sure everybody knows, that requires you to prove effectively economic lost before you can claim damages for distress. None of the claimants in this case could prove any economic loss and so if section 13 was read literally their claims for damages under the Data Protection Act were bound to fail. Incidentally, the civil claims

[14] The judgment can be found at: http://www.bailii.org/ew/cases/EWCA/Civ/2015/311.html

brought in the United States over the same issue all failed - were all struck out - because they were unable to prove economic lost. It's obviously a very different set of laws but crystallized on the same issue.

The central issue in this part of the judgment for the Court of Appeal was whether or not section 13 covered not just economic damage but also what was referred to as moral damage, in other words distress, damage to reputation and so on. It was accepted by everybody that, read literally, section 13 had that effect. There's no way around it. Section 13 required, as a necessary condition, a proof of economic loss. There was an interesting debate as to whether under *Marleasing* you could strike words out,[15] whether you could strike whole sections out. Well I thought that was impossible. The Master of the Rolls said to me "why?". I was slightly at a loss as to how to [respond]. Well it's absolutely obvious, you can't go striking out bits of Acts as a process of construction. In the end, he accepted that. So that route was closed but what the Court of Appeal accepted was that, first of all, the word "damage" in the Directive in Article 23 covered both material and non-material damage. They based themselves partly on other decisions concerning other Directives and concerning the meaning of the word damage in the Treaty but partly on the general point that actually what the Data Protection Directive is about is protecting privacy rights, autonomy, dignity, not economic rights and it would be bizarre if your rights are interfered with but you had no remedy because only economic damage was protected. So they got to the position of saying yes damaging in the Directive does mean moral damage as well. Yes section 13 doesn't properly reflect the Directive so what do we do about it? We can't construe it out of existence. The answer is, we disapply it because of Article 47 of the Charter which provides for an effective remedy. There is no effective remedy. EU law takes precedence so we disapply section 13. Effectively, what they've done is the process which is done in constitutional courts I think everywhere in, I always say this, everywhere in the world apart from England and New Zealand. I may have missed somewhere out. But in other words they strike down laws which are incompatible with more basic and fundamental laws and effectively what they've done to strike down section 13(2), which has a massive practical impact, because what that means is that now in respect of data protection breaches for the first time you can unarguably claim damages for distress whether or not you suffered economic loss. Now, does that demonstrate Orla's point made this morning about the Court's being, I think she mentioned *Vidall-Hall* in passing as an example of the courts being more activist in this field. I suspect not certainly in relation to the English domestic courts, but I do think they are becoming more constitutionally aware partly because the Human Rights Act and more aware so applying the Charter doesn't now seem something outrageous and foreign as it might've done even five years ago. That they think that's something that if that's where the law takes them that's where they go. So the decision is also important because there's an important discussion of what constitutes personal data. It was mentioned this morning that there's not much discussion at that in *Google Spain*. There's actually more discussion in *Vidal-Hall* and in particular they accepted that you didn't have to name someone to identify them. I mean an obvious point, but Google argued to the contrary. So that's the first thing I want to deal with.

The second issue is one that's arises out of *Google Spain* and it concerns the question about what you do about systematic problems because *Google Spain* envisages, the paradigm case, is reporting an individual URL. Mr Costeja reports that there's a URL which links to La Vanguardia and contains this information and ask Google to de-link it. But what happens if you get the not atypical situation where someone is putting large amounts of the same personal data onto the Internet - Google groups, or Facebook or onto YouTube or whatever. Is the position that you have to notify Google of every single URL or can you get Google to take some more automated procedure? That problem arose in the case of *Hegglin*,[16] which I noticed in the notes for this event was mentioned by David, and in *Hegglin* there was some unidentified person who, we never worked out what was behind it, but they were putting on all kinds of places on the Internet thousands and thousands of postings which said that Mr Hegglin was a criminal,

[15] The judgment can be found at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61989CJ0106

[16] Hegglin v Persons Unknown [2014] EWHC 2808 (QB). The judgment can be found at: http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWHC/QB/2014/2808.html&query=daniel+and+hegglin+and+v+and+persons+and+unknown&method=boolean

bastard, Nazi, paedophile, and so on. They went into a lot of detail about his [alleged] Nazi, paedophile, criminal activities, so every time you did a Google search on him these were the first ten results, was this abusive material. We originally used the procedure under the Google Spain, what Google called the *Costeja* procedure. Google, on the first occasion, took fifty eight days to respond. By the time the case was almost due in court, they were responding in six hours. I'm sure that was a coincidence. The issue in that case, and the case was settled so it was never resolved - the issues also come up in other cases - is whether Google can be compelled to introduce an automated procedure for detecting particular groupings of text or particular images and blocking those proactively without being notified of individual URLs.

Hugh Tomlinson, 27 March 2015, University of Cambridge

That itself gives rise to an issue which I don't think has been mentioned today but is a very important issue as to the relationship between the e-Commerce Directive and the Data Protection Directive. Google's position is that the e-Commerce Directive prevents courts from making proactive orders so that they have to block particular images or particular groups of text. The position of the people who brought the claims against Google is, if you read the e-Commerce Directive it says - this doesn't apply to data protection. Now that's an issue which has not been litigated in any court in the EU, save for one case in the Italian Court of Cassation, pre-Google Spain, where the reasoning, if I can dignify it with that word, occupies half a page and may be easier to follow in Italian but in the English translation it's impossible to work out what they mean. They have said, for reasons which are entirely obscure to me, that the e-Commerce Directive despite its express words takes precedence over the Data Protection Directive and therefore Google don't have to take things down unless they have knowledge of them. Unless you identify the particular URLs. That's an issue which just as a matter of practicality is going to come up more and more because it's one thing. Another problem is images. For example, the well-known case of Mr Max Mosley. There are their images related to him which are all over, extracted originally from the video taken by the undercover person working for the News of the World, that pop up all the time. What he wants is an active procedure. As some of you may know, he brought proceedings in France and in Germany where both the French and the Germans courts have

made orders effectively requiring Google to take proactive steps. This is not a *Google Spain* question, this is a privacy question, but he's now brought proceedings in the English courts under *Google Spain* seeking similar sorts of orders. How those cases will ultimately pan out? The German case has just gone on appeal and judgment is due in five weeks time, I think. The French case is also going on appeal and the English case is continuing. But those are practical issues that arise once the courts in the EU exert jurisdiction over Google as they plainly can as a result of the *Google Spain* decision.

JAMES LEATON GRAY

Controller, Information Policy, BBC

Alright good afternoon to you. I am now going to break the first rule of speaking at a conference and contradict the Chair. I'm going to break it in the beginning which is an even worse way of doing it which is to say I just need to correct I'm I no longer Head of Information Policy and Compliance. Google gave you the wrong information. I was until last year Head of Information Policy which is indeed in charge of data protection and freedom of information. The reasons I point this out is two-fold. First, we are the BBC and we like accuracy and secondly because I've left that behind and I am now sort of reflecting upon that ten years leading that team. I've been put on big data which I'll come back to in a moment or two. I'm soon going to be leaving the BBC and so most of what I'm going to say today is going to be my personal reflections upon this as I move out into a new era still sticking, I hope, in the privacy sphere.

Firstly, a couple of points and I promised to David that I wouldn't I wouldn't spend too long in this session reflecting too much on the last session and around a media response. I do think there are just two things I would say in terms of the Article 29 Working Party response as opposed to how Google is implementing it. From a media perspective, we think that there are some problems with the Article 29 Working Party suggestions and indeed sometimes the way it is implemented by Google. There is an issue around transparency and I think that continues to be an issue. Actually I will pick up on my own personal views in a moment. If the publisher doesn't know, and the Article 29 Working Party suggests that in most circumstances the publisher does not need to know, that the URL has been taken down then actually how can Google be making a properly informed judgment? There may be issues that the data subject has raised which the publisher has counters to. Those facts need to be known. There isn't a balance there. This comes to the date subject who has the right to appeal but the publisher doesn't according to the Article 29 Working Party because the publisher isn't appealing under the Data Protection Act or under the Directive. Again, there is an imbalance. I'd like to come back to this point about balance going forward because I do think actually we are in danger of regulating and legislating in silos and ignoring the fact that other silos that are significant and have impact in this area.

Also, I just think that I think there's a slight danger. Willem suggested there's never been a problem censorship except as in the vast majority of territories the publishers are not being informed the URLs been taken down, we don't know whether there's a problem of censorship because the publishers don't know that it's happened. That is in essence a societal problem that I think we need to tackle and it's back to this point [that] you can't have a fundamental right being judged unless you actually are balancing it.

So, that's the BBC position. Now this is all down to me. So when I get the rest of it wrong, you can just shout at me instead. I do think I'm nervous of data protection authorities being the bodies given the responsibility to make this balance particularly reflecting upon freedom of expression, section 32 in the DPA, and more broadly. Data Protection Authorities are there to enforce a fundamental right, they're a very important part of the mechanisms but they're there to enforce one right. How can a body that's set up to enforce a right then balance other rights that it has no responsibility for? When I said this to an audience in Brussels recently a member of the CNIL said: well we deal with all sorts of industries all the time, very very important industries. We can do all sorts of balances. Yes, you

deal with every industry pretty much. There are very few industries perhaps apart from chicken rearing that doesn't involve personal data. But I do think that there is essentially a problem here that actually I'm not sure a regulator for one right is the appropriate body to be balancing other rights. Eduardo from the second panel and I have an absolute agreement here. I don't think that actually Google is a data controller. Now I take Chris's point if it's not a data controller what is it etc.? Well my answer to that is at least when it comes the new Regulation they need to put something in that makes sense in the modern world but it's a bit too late to start. So we've got a mainframe idea being translated into the new Regulation which will be Web 2.0. Frankly, the idea that it is up to date is ridiculous. But the data controller has certain implications - how you do a subject access request to Google? Well, I suppose you type your name in. But data minimization? I don't know about you, but I don't won't a search engine that does data minimization. Surely the point is it's meant to go out and find stuff? Data minimisation - I could do that myself. So there are contradictions and we're back into this disconnect between the law and reality, which has been mentioned already.

James Leaton Gray, 27 March 2015, University of Cambridge

Now I do actually think, by the way, that I was accused in that same panel up not being in favour of privacy. I've been the BBC data protection officer for ten years. I believe passionately in this stuff but I do think that has to be a balance and I think where that balance comes will be in the pragmatic. We can't get rid of the concept of controllers and data processes or introduce a third route which should seem to be the sensible thing to do in the new Regulation. We will be stuck with it. But the pragmatic solutions have to reflect the real world.

My other problem with the judgment and this is also true in - there's a case that I don't think has been mentioned so far today – *Telekabel*,[17] an Austrian case, which went to the CJEU. Where what we have is what I think is a very dangerous pattern of the courts and society, I don't just blame the courts here, but the courts and society effectively outsourcing judgments. We said to Google actually there's a lot of really difficult stuff to balance here, freedom of expression, personal rights - you go away and do it because we haven't got time in the courts and we don't spend the money. Getting a commercial organization, however well-meaning - I like William, I know him very well, I think he does a terrific job - but should he be doing this job? I question that. *Telekabel* has basically been told to go away and sort out IP infringement in Austria. Yeah, good luck with that. But why are we doing this well because actually we don't have a mechanism to deal with it accurately ourselves. We can't get David to do it: he's got enough on his plate already. So it seems to me that that as a society we are making more and more calls upon groups to do things because actually we haven't got the resources to sort it out ourselves. I think it's a dangerous route to go down.

So there is this balance point. I did promise to talk about the other internet players because I do think it's quite important. This is where this balance point comes back. I'll come back in a moment if I have time to media archives but social networking, online forum [and] the blog posts. Some of you may know a case on the freedom of information side of my former life Sugar v BBC[18] which was about how widely do you define journalism, art and literature. What is the definition? That was in relation to freedom of information but clearly the same phrase appears in the Data Protection Directive and in the DPA. When you look at nearly all the jurisprudence we are told to interpret it widely and yet there's a contradiction here because we're also told to interpret the data protection widely. So we have got these two wide definitions which overlap in the middle and I don't think we've really got our heads around this. The right to be forgotten I think does, as David has suggested, apply to a large number of internet players here. I don't think it's just search engines. I think the blog post is one example. I think social networks, online forums but we're not even thinking far enough ahead. I've been doing some thinking around IPTV in this last year looking at Big Data and Internet Protocol television. Once your television set is effectively a computer, search is not going to be something you sit and type in. You are going to talk to your television set. I mean sometimes you do that anyway but that's normally shouting and it's not quite the same thing. You're going to say "get me the news!" Whose news? What news? There will be an algorithm. It will probably be constructed by the set manufacturer. It will be Samsung's news algorithm. Will we know that actually the section from La Vanguardia, or from the New York Post, or whatever has been removed? No we won't. I do think that although, as Julia in the second session said, this is statistically insignificant - yes it is the number of major news items that might be removed is going to be statistically

> *We already have the majority of large companies in this space, the American companies, genuinely not understanding where we are coming from. These are people for whom the First Amendment is absolutely ingrained. We are going to make all those conversations significantly harder. Now that's not problem in itself and I don't think that should be a reason for not doing it but actually if you start thinking in a globalized world I do think that we are in danger having a conversation with ourselves rather than the rest of the world.*

[17] UPC Telekabel v Constantin Film (Case C-314/12): http://curia.europa.eu/juris/liste.jsf?num=C-314/12

[18] The judgment can be found at: http://www.bailii.org/uk/cases/UKSC/2012/4.html

insignificant - but socially I would contend it is massively significant and I think we have to be careful about wandering along this line and again forgetting the balance. This is Article 8 versus Article 10 or, if you want the Charter, 7 and 8 verses 11. And I think these are not incompatible. I think that a balance can be made. But I would contend at the moment that the two sets of arguments are being put in opposition and are not actually being balanced. I suggested something akin to this in Europe and it was suggested that somehow I haven't read the judgment. I've read the judgment. I would contend that putting the word "balance" in a judgment does not make a judgment balanced. Now I fully accept that coming into a room full of lawyers that's a dangerous statement to make but I do think actually it's important. I think that wasn't enough balance made and I think that's because actually to be fair to the CJEU the reality was that they had to make a call on that set of circumstances. Were they really going to lift up the rock of freedom of expression at the same time? I don't think they would have been finished now. So we've got over here the right to publish and we've got over here the right for the individual. Well that's fine but we're going to have to bring them together. We're going to have to do that sooner rather than later I would contend.

I've already said that I think this is a Directive for the mainframe - the Regulation web 2.0 – and I think we are not going fast enough to look at the future. The direction of travel has been mentioned by David: the culture point. I actually am concerned about the direction of travel not just because I think freedom of expression is being underweighted in this, although I do. But I also think that it is going to create further and further problems. The harmonization point that the Regulation is pushing toward is going to make this more difficult. We already have the majority of large companies in this space, the American companies, genuinely not understanding where we are coming from. These are people for whom the First Amendment is absolutely ingrained. We are going to make all those conversations significantly harder. Now that's not problem in itself and I don't think that should be a reason for not doing it but actually if you start thinking in a globalized world I do think that we are in danger having a conversation with ourselves rather than the rest of the world.

You are then back to what is and is not appropriate inside individual territories inside Europe. For those of you who don't look up the Wikipedia case in Germany.[19] I can't for the life of me remember the name of the case but effectively two people who were convicted of the murder an actor went to Wikipedia and tried to get their names removed from the Wikipedia article about that actor. They didn't deny that they had done the murder or deny anything about it. They wanted to get on with their lives. Again, a perfectly reasonable balance to be had but actually there is an element then of rewriting history. And we have to as a society to work now what we want to do about this. When we come to these new media players. When does a blog post trip over into what I would call the "casual vacancy" effect.[20] I don't know whether you saw the dramatization but for those you didn't one of the things was a scurrilous website that was sort of telling the truth. I get very nervous. I heard earlier today when we are taking about well those circumstances where defamation or inaccuracy. Well actually what's one what's the other? My background before I got into privacy was as a political journalist. My exit from the BBC will be running an OB [outside broadcast] for the general election. I'm being let loose with a toy cupboard again and I'm looking forward to that. But when you try and apply those kind of absolutes that only the law can - in court when you look at the full set of facts. And you say we are going to do this on the fly, we're going to do this, we're going to outsource it to commercial companies, or we're going to have poor old David again at the ICO deciding whether that is or is not an accurate statement. I don't think that is appropriate and I think we've got to get that balance right.

So I've only got about one minute left I think. Is there a way around? Yes I think there is pragmatically. What I've been doing for the last year is preparing a thing called "My BBC" which is going to be going live in the autumn and is actually about personalization. The only way you can work personalization is by getting a large amount of data about people. You can do that. You can take people on board. I genuinely believe you can't make big data privacy friendly and I think they are involved in the process of doing so. But even when you do do it pragmaticly you're

[19] See http://www.theguardian.com/technology/2009/nov/13/wikipedia-sued-privacy-claim

[20] See J K Rowling, The Casual Vacancy (2012)

going to end up with some further conversations which we need to be having. What about exhaust data? What about data that you don't even know you've created just by wandering around the internet? Is that your personal data? It could describe you in certain circumstances. How do you define when it's going to be put into an anonymized form? Created data, the data that is going to be created by services for you at your request in order to supply you those services. Is that still personal data? Where does the algorithm itself become personal data? These are issues that need to be tackled and I do think that we need to look at them but we need to look at them in terms of the balance of the privacy right which is vital but some the societal benefits that the individual and society can gain by having that privacy right notched down or notched up but we need to have the conversation. We need to have it in a broad sense and we can't just have it in terms of a single judgment.

FLOOR DISCUSSION, QUESTIONS AND RESPONSES

Question: A delegate asked Mr Gray why he thought data protection authorities cannot balance data protection and freedom of expression. He further asked what should happen where a data controller does not believe the data subject. A further problem was that indexes may re-index results automatically and the solution for that must lie in technology.

Mr Gray answered that, philosophically, he did not think it right that an organisation whose purpose is to enforce one right, to enforce data protection, to be responsible for striking balances between that right and another, freedom of expression. It did not mean that they were incapable of it. Judges do it but they do not have responsibility for one particular right over others. There is no regulator for Article 10 trying to do the equivalent. In this instance there is a regulator on one thing but not for the other.

Mr Tomlinson argued that Ofcom regulates broadcasters and does balance Articles 8 and 10. The idea that a regulator has a closed mind is quite strange.

Mr Smith added that the regulator's role was to fulfil its obligations under the Data Protection Act which involve balancing a whole range of different rights.

Dr Erdos added that the law is predicted on the notion that regulators must intervene where something is done that is against someone's rights. Yet publishers do not have a right in law to be indexed in Google's index, whereas people do have a right not to have their data protection rights violated. This is the crux of the legal inequality between publishers and data subjects.

Question: A delegate asked whether big data could be privacy friendly and how that could be done.

Mr Gray answered that it was about transparency and control. This goes beyond consent to give control. Control is more significant that consent. If it is understood that it is a value exchange it makes it more privacy friendly than a tick box consent where information is then sold on. The forms should make it clear what the data is wanted for and why they should give it. It is about making forms clear. He thought you can do that.

Question: A delegate asked about the rights of delisted media. She noted that this was part of a question about procedure and delegating decision-making down to a private company. She voiced fears about delegation to a private company and the lack of voice for private publishers, other than the republication of delisted articles by those media.

Dr Erdos considered that there were legal problems in data protection law around notification to publishers. Google, and other search engines, had a strong economic and broader reputational interest not to delist too much information. This encourages a balance of sorts because the entity does not want to go into too much delisting. A trusted relationship with media outlets might be a fruitful way forward, if it abides by the legal requirements, but simple unsafeguarded notification was problematic.

Mr Smith commented that he had sympathy with the argument as put. Third party publishers had an interest which was not present in most cases that come to the ICO. He added that he had more of a problem telling them after the decision to delist has been taken, where it does not add to the decision making, but they could have a say in the process before that.

Mr Tomlinson added that often the publisher is not responsible like the Guardian. Giving them notice is problematic. There needs to be a proper process for responsible websites like the BBC or the Guardian. If Google is delinking the Guardian should delink it too.

Question: A delegate asked about the rights of third party contributors.

Mr Gray answered that he had particular concerns about the future that people would all go to the same site for news, news that came from an algorithm or link. This trend was far truer of the younger audience. Their freedom of expression in a small way is constrained.

Mr Tomlinson added that if Google was operated by the State it would be possible to argue that Article 10 was infringed by closing links. The Strasbourg jurisprudence does not make any radical distinction between public and private bodies. The State may well have a positive Article 10 obligation in relation to this. If Google exists and has a monopoly there may be Article 10 issues.

Question: A delegate asked to what extent the Charter and effective remedies could enable a remedy to be developed. Could Article 47 of the Charter be used in interesting ways.

Dr Erdos noted that he was surprised that in the Vidal-Hall case Hugh argued that Marleasing would not get him where he needed to go, and not surprised that the Master of the Roll said why not, because decisions such as the rape shield case the Human Rights Act indeed found it possible to interpret as far as striking out whole portions of legislation and he would have thought that in EU law at least as strong a duty would apply in terms of indirect effect which would involve striking out as long as the overwhelming purpose of data protection is not undermined by that. But they have done it via the Charter. He supposed that had a range of other potential possibilities. For example, David Smith mentioned that under our Act you only have a right to object if you show unwarranted damage or distress. That reflects to some extent Article 14, the right to object on compelling legitimate grounds. But there is also a right under Article 12 to simply have erased data which is illegal under data protection. The right to erasure does not need you to prove any kind of damage, any kind of distress at all. If it is illegal and it relates to you it should not be being processed. That is what Article 12(b) says. There seems to be the potential to read down threshold for our Act's right to object in exactly the same way we saw as regards damages in Vidal-Hall. He could see an argument running there. Generalised search engines should not be processing data which is illegal. If they have the technical capability to prevent that processing he would have thought they do have responsibilities to take semi-active steps.

Mr Smith added that the next step might be for controllers to be much more proactive in taking down inaccurate data. The Northern Ireland case took exactly that view with Facebook. Facebook was requiring individual URLs. The court said that was wrong and it had to be much more proactive.

Question: A delegate asked whether the first step is to ask the Guardian to remove information as it was the information not the link that was the problem.

Dr Erdos responded that under data protection law if a controller amasses data from third parties it can't refer data subjects elsewhere without looking into the legality of its own processing. Google is a controller with distinct responsibilities.

Mr Gray commented on the difficulty with new players, such as blogs, where the responsibility of the writer or the platform raised difficulty questions of who is the controller.

Dr Erdos noted the concept of joint control that might apply in some cases.

Question: A delegate asked the panel for their thoughts on the implications of Google Spain for Twitter and Facebook.

Mr Tomlinson noted they were both established in the EU.

Mr Smith said they could not evade data protection law. Facebook was in Ireland and subject to the Directive. It has never tried to suggest otherwise so you do not need to go down the establishment construction. Other laws apply. It is not necessarily Irish law. There is a difference between which is the Data Protection Authority whose jurisdiction it falls within, which is Ireland, but it is processing not just in Ireland so it is subject not just to Irish law but is subject to other laws as well. The Netherlands DPA was taking up the question not because of a legal analysis but because it is under political pressure to do so. It has been raised in the Parliament, citizens are complaining and that is what drives it. Data Protection Authorities are about protecting people's person data. That is the aim. That is the target. And data protection authorities interpret and use the law in a way that helps them do that best. It is not necessarily always the law that drives it.

Mr Tomlinson added that assuming they were established then they are controllers and all the consequences follow.

Dr Erdos commented on the enforcement gap and added that until that was sorted the reality would be a dysfunctional system.

SESSION 4: JURISDICTION, APPLICABLE LAW AND BEYOND AFTER GOOGLE SPAIN

CHAIR: NORA NÍ LOIDEAN, UNIVERSITY OF CAMBRIDGE

Background: The Google Spain judgment found that the Google search engine was subject to Spanish data protection law since its processing was "inextricably linked" and therefore took place "in the context of" its Spanish advertising subsidiary. Given that the Directive is clear that "where the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with obligations laid down by the national law applicable" (Art. 4 (1) (b)), this finding is difficult to square with the insistence by many European Data Protection Authorities until recently that Facebook only need comply with Irish law and not the data protection laws of other EU Member States. This issue was challenged (at the time unsuccessfully) by regulators in Schleswig-Holstein. At the same time, even though the Court in Google Spain refused to discuss whether using a national domain name and/or using robots to access European websites would trigger EU law on the basis of a "use of equipment", the judgment also opens up the possibility for many activities taking place entirely outside the EU being subject to EU data protection requirements. These and other complex but important jurisdiction and applicability issues were explored in the last panel. This panel also touched on the likely future shape of the law under the proposed General Data Protection Regulation, especially but not only vis-à-vis applicable law and jurisdiction.

PROFESSOR DR JOHANNES CASPAR

Hamburg Commissioner for Data Protection and Freedom of Information

Well thank you for your nice invitation, David, to Cambridge. It's a great pleasure to be here and to speak to you. For a data commissioner in Germany, it's always a great thing just to go elsewhere and try to push the idea of data protection throughout Europe. Well, I want to give you a legal assessment about the problem of the applicability of national data protection law. As you see this is the structure of my essay and perhaps it will help you to get a notion about that in this short lecture. It's a question which goes on at another level I think. We heard just now about the implications of the Google Spain decision for search engines but now we're on the point where we go on another level where we can see what great impact this decision has for all kinds of platforms on the internet, for all kinds of services. But, as the time is precious, let us begin.

Introduction on the historic adjustment on the right to forget:

Without exaggeration one can call the decision of the European Court of Justice in the case of *Google Spain* historical. This applies at least for the central part of the verdict that the judicial derivation of the so-called right to be forgotten, better called the right to be delisted, a right not to be found so easily. The ruling brought the shocking evidence to Google and other companies that from this point on they were seen as responsible data controllers by operating internet search engines. They also had to realize that they can't escape European data protection provisions even if they are set up outside the EU but have an establishment in at least one of the Member States. The ruling of the Court of Justice therefore not only bolsters the privacy rights of people affected by the use of their data on the Internet. It also clarifies the scope of applicable national data protection law and helps to safeguard the data protection rights vice versa parties which play on grounds where data protection normally is an alien concept.

Professor Dr Johannes Caspar, 27 March 2015, University of Cambridge

The content and range of the decision:

The European Court concludes that national data protection law is applicable if the activity of an establishment in the specific Member State is economically linked to the controller. This applies even in cases where the regional establishment in the Member State itself has no active part in processing personal data of the users of an internet service. It is sufficient if the activity of that establishment fosters, economically, the data processing of the holding company. Now there is a short way from the Google case to another global service provider which has its German establishment in the State of Hamburg. You know of which kind of service I'm speaking. It's the biggest social network - Facebook - that in the past has given several reasons for taking the data use policy under close scrutiny to the Data Protection Authority of Hamburg. Some examples. The first such reason was the Friend Finder, an

aggressive advertising strategy of Facebook to increase the number of their users. The second one, another similar case, is the face recognition technology Facebook used to suggest whom to tag on photos uploaded by users to the network. This was introduced without asking the data subject effected for their informed consent. After we opened an administrative proceeding against Facebook, they decided to discontinue the features throughout Europe. Currently, a change of the data use policy of Facebook effective at the end of January 2015 led to new investigations not only by the Hamburg DPA but as well in the Netherlands and Belgium and we know that since last week also in France and Spain. The announcement that Facebook may share information about their users within the Facebook family for more or less undefined purposes is at least disturbing. The legal ground for transferring data between these different companies cannot be seen. Facebook therefore must clearly commit that there will be no unauthorized exchange of data, especially keeping in mind the weak privacy standards of the US companies in the hands of Facebook such as WhatsApp or Instagram. One can also count here the network advertiser Atlas. Facebook has argued for quite a long time that for European users the responsible controller, it is not Facebook Inc, located in California, but rather Facebook Limited in Ireland. From that they come to the conclusion that the Irish Data Protection Commissioner would be the only competent DPA. Despite this position, Facebook in the past was willing to answer our questions more or less to our satisfaction. Not so now. Facebook refused to give answers to our questions concerning the new data use policy. They returned to the argumentation of missing competence and the non-applicability of German data protection law.

Our legal position:

Until now, the competence issue in Germany has not been solved. There are two dissenting court decisions in Germany. The Administrative Court in 2013 denied the applicability of German data protection law. On the other hand the decision in January 2014 [by] the Berlin Court of Appeal for private law argued that the national data protection provisions are applicable for Facebook. Considering the current decision of the European Court the key question of applicable law under the framework of the Data Protection Directive must be addressed anew. The central provisions apply in the Google Spain decision concerning the applicability of national laws [is] Article 4(1)(a). The Article provides that each Member State shall apply the national provisions where "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory several Member States, he must take the necessary measures to ensure that each of these establishments comply with the obligations laid out by the national law applicable". The clear notion of Article 4(1)(a).

To estimate the extent of the application of the national data protection law one has to analyze the key term "establishment" and the scope of the relevant activity. The Court refers to recital 19 of the Directive which states that "establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements" and that "the legal form of such an establishment, whether simply branch or subsidiary with the legal personality, is not the determining factor". The Court of Justice makes it clear that this does not require the processing of personal data in question to be carried out by the establishment concerned but only that it be carried out in the context activities of least of this establishment. In the case of the Google search engine it is sufficient that the establishment promotes and sells advertising space making the service more profitable. The Court of Justice explicitly develops its wide interpretation on the background of processing of data which is operated by an undertaking that has its seat in a third state but has an establishment in a Member State. Now what does this mean for those cases in which the controller claims to operate not in a third state but in a Member State of the EU? The multiplication of different national regulations is anticipated by the Data Protection Directive. It states that each controller has to ensure that the national regulations have in each case been followed. Recital 19 of the Data Protection Directive addresses this issue. A quotation "when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations of those by the national law applicable to its activities". The decision of the Court of Justice therefore, this is my opinion, is also then valid for controllers who operate within the EU. By contrast, Facebook which shares its main European establishment in Ireland argues that the Directive would aim to ensure a common level of privacy protection standards within the EU and harmonise

data protection laws to establish a consistent internal market for internet services. The Data Protection Directive in order to ease the flow of personal data aims indeed for the equivalent level of protection of rights and freedom of individuals with regard to the processing of such data in all Member States. This is recital 8. It is clear that the interpretation of the term establishment by the Court of Justice intends to counter controllers trying to escape the obligations and guarantees of the Data Protection Directive and safeguards the effective and complete protection of fundamental rights and freedoms of natural persons. An interpretation of the scope of applicable law must therefore consider that with Directive 95/46 the European legislator sought to prevent individuals being deprived of the protections guaranteed by the Directive and that protection from being circumvented. A quotation from the European Court. Even if one follows the argument of Facebook on the harmonizing intent of the Directive, the right interpretation of the term establishment by the Court must therefore be also relevant for the data controller in Member States where the implementation of the Directive itself is deficient or/and the enforcement of national data protection is at least much less effective than in other Member States. As a result the controller whose strategy is to seek for lower levels of data protection in third States as well as in the EU must at least face this situation that he is obliged to the relevant data protection standards of Member States where its own branches or establishments are running an office.

I come to point four: implementation and law enforcement in Ireland:

Whether these requirements for the application of the principles of the Google decision are fulfilled in the case of Facebook Limited in Ireland must be examined. Here is not the place and the time for a final even but let me in short provide an initial assessment. As an example I will pick the enforcement of proper consent as a legal ground for processing data. As mentioned before, Facebook in 2011 implemented automatic face recognition to identify people in uploaded photos and attribute these to the users in question. Facebook itself when introducing this function did not inform the users that their faces would be biometrically evaluated. Under the pressure of growing resistance especially among consumers and Data Protection Authorities, Facebook prominently pointed the user to the facial recognition function and the possibility of deactivating it. Facebook was of the opinion that it had done all that was necessary to obtain the consent of those affected. True to the motto: if you don't you deactivate then you consent. The user's reaction not to deactivate the facial recognition function was regarded as a consent. We clearly pointed out that the failure to perform an action - deactivating - may not be interpreted as consent on the part of users. Consent from those affected is required by European as well as data protection law: unambiguous consent. This view was, by the way, repeatedly communicated by the Article 29 data protection group in its opinions on the processing of biometric data entry requirements for valid consent. That opinion was not shared by our colleagues in Ireland. In the first Irish audit report, they accepted Facebook's argumentation that users give their consent to all of the network's conditions of use including the guideline on data usage and that this provides substantive legitimation to the collection of user's biometric data. A quotation from the Facebook Ireland audit report 2011: "Our consideration of this issue must also have regard to case law in Ireland regarding the use of biometrics. This case law has not considered that the processing of biometric data requires explicit consent." Further quotation: "For the reasons outlined above further notification in relation to the current deployment in the future is not strictly legally necessary under Irish law". This opinion ignores that with the opt out feature Facebook does not fulfil the requirements of the EU Data Protection Directive. Article 2(e) provides that the data subject's consent shall be "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". The EU Article 29 group opinion in 2012 on facial recognition[21] in online and mobile services approves that the quotation "In this context, consent for enrolment cannot be derived from the general users acceptance of the whole terms and conditions of the underlying service unless the primary aim of the terms of the service is expected to involve facial recognition". It took quite some time for Facebook to accept this legal opinion. Only after the opening of administrative proceedings Facebook took the possibility and closed down the facial recognition function in Europe. The function of facial recognition was discontinued and the

[21] This opinion can be found online at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

biometric data was deleted. This example shows and demonstrates one of the differences between the Irish Data Protection Act and the EU Directive. Deviating from the EU Directive, the Irish Data Protection Act has no binding legal definition of the term consent. This proved deficient implementation of the Directive and documents the gap between the provision of the EU Directive and the Irish Data Protection Act. This gap should have been closed by interpretation of the legal term "consent" by the Irish Data Protection Authority in the light of the European Directive. Referring to Irish case law certainly in my opinion is inappropriate. The question of free and explicit content is crucial for the other evaluation of the data use policy of Facebook which became effective just in January 2015. Has Facebook by issuing the new privacy policy acquired consent of their users that legitimates the processing of personal data from a European perspective? This is more doubtful.

I come to the conclusion:

The EU General Data Protection Regulation has been discussed on the EU and on the Member State level since 2012. It aims for structures and future data protection law not only for privacy rights but also towards a homogenous procedure of cooperation and law enforcement between different national supervisory authorities. The principle of the one-stop-shop should accomplish that only one Data Protection Authority is competent for a data controller throughout the EU. Against the background of the above, it is of great importance that the exclusive supervisory responsibility of the authority at the location of the headquarters of the data controller must not lead to forum shopping of a major Internet company. Otherwise you might face a race to the bottom in the protection the privacy in the EU. The General Regulation therefore has defined clearer and transparent procedures which provide effective provisions for the law enforcement. Consideration should therefore be given to the question of arming those supervisory authorities with particular rights for the case of the leading authority should remain inactive. That last view on consent, the actual proposal of the Council of the European Union raises doubts whether the procedure of the one-stop-shop will be effective enough for law enforcement regarding also the consent proposals of the Council in chapter two of the General Data Protection [Regulation], falls back below not only beyond the proposal of the Commission but also beyond the EU Directive itself. Instead of an explicit consent required by the proposal of the Commission mere unambiguity shall be sufficient. That we open the way to opt out solutions which are incompatible with the right to personal self-determination of the user. The essential requirement for the ongoing debate on the data protection regulations is to implement the definition which states that consent of the user always be given explicitly. The Data Protection Regulation must learn from the process of the European DPAs to enforce the fundamental rights to privacy especially against data use policy of global players like Google and Facebook.[22]

BRENDAN VAN ALSENOY

KU Leuven

I'm going to start by also thanking David and congratulating all the organizers of this panel for this very stimulating event in this really, really wonderful location. So that's just the academic way of saying I envy you, David.

I'm Brendan Van Alsenoy — I'm not Marieke Koekkoek, as I hope you may have guessed. What I'm going to present today is really a product of our joint work and I wanted to make sure that she got due credit for it.

So when we think about internet and jurisdiction after *Google Spain,* there's really two sets of jurisdictional questions that come up. The first is the one about prescriptive and adjudicated jurisdiction, and that's very much what Johannes Caspar was just talking about. So I'm not going to get into that here. What I am going to talk about it is the geographical scope of the implementation. So should a search engine provider, when it decides that a request

[22] A revised version of this paper reflecting Prof. Dr Johannes Caspar's current thoughts following discussions with different stakeholders on the topic can be found in J Caspar, "The CJEU Google Spain Decision" (2015) 9 Datenschutz and Datensicherheit 589.

to be delisted should be granted, how far should its implementation stretch? Should it implement only local search results or should it extend more widely, more globally? So, as we heard today, Google's current approach is to go simply local - it's mainly a domain-based approach. If you type in google.com, they will gently steer you back towards whatever is the appropriate domain name for use - so here it would be on Google UK. But at the bottom of the webpage, there is still this button that suggests you want to switch back to google.com.

One of the main concerns with the Data Protection Authorities about this approach is that, well, if you make it that easy, then it's not really going to offer much effective protection. So the Article 29 Working Party has come out and said: well, actually you have to implement a ruling on all relevant domains, including .com. Otherwise it's simply not effective. Now, the critics - there's a lot of criticism over this position because, you know, isn't this just the EU imposing its values onto non-EU countries? I mean, this right to be forgotten is found by the European Court of Justice - should we actually be wanting the court's ruling to stretch that far? So the debate so far has really been quite polarized. It's been kind of simplistic, and so I apologize, my next slide was also going to be a little bit simplified in portraying the two positions.

So the first side is what I would call 'Team Global'. They advocate for global implementation of the ruling, like the Article 29 Working Party, to say that otherwise it's not effective and complete, and anything else is too easy to circumvent, right?

Then there's the opponents, call them 'Team Local'. They would like to see search results only modified in the EU; either through the domain base approach or by detecting the geographical origin of the search query, and tailor results appropriately. They like to talk about the power of the default.

We heard today, one of the statistics that Google likes to present is that ninety-five percent of its users, if they type in google.com, they get back sent back to their local version of Google and they'll stay there. Now, interestingly, this statistic concerns all of Google searches - it does not just concern name-based searches, and as you also know, at the bottom if you do a name search within the EU on a person, it will show: some results may have been removed. It won't take you very long to catch on and go to another site. The other argument is the lowest common denominator argument where they say: well, you know, the EU, it's a very democratic and very enlightened system of government, and so, you know, we might recognize that it wouldn't be the end of the world or the end of the Internet if it expands beyond just the EU. But what about if other states start to do the same thing. What if North Korea decided that, you know, every link to its supreme leader should be taken down?

The sad thing about polarizing the debate the way I just did it is that actually both sides have valid points, and both sides have something to learn from each other. What we did in our paper was try to analyse from the perspective of public international law which side is right and which arguments could be made in favour of either approach.

So under public international law, territoriality is the primary basis for jurisdiction. A basic function of a sovereign state is to determine by law what forms of speech and conduct are acceptable within its borders. A corollary of this principle of territoriality is that you have to respect other states also as being sovereigns within their borders, right? Do unto others as you would wish they'd do unto you. But still even though this is the main foundation of the public international law jurisdiction, it's not the sole foundation. After a while, people realize that activities that take place in State A impact interests in State B. So, particularly in competition manners, we have this thing called the 'effects doctrine', which says if there is a substantial effect within the state's territory, it can actually justify regulation of activity which is taking place abroad. Actually, I think that's that very same principle that underlies the application of Article 4(1)(a) in the *Google Spain* case; there's talk of an establishment but really, the connection, the territorial connection that the establishment offers is just virtual. I mean the processing - it's admitted - is taking place mostly outside of the EU territory.

So a problem with a concept like 'effects' is like, when does a particular activity taking place in another state affect your state? Could it be just any effect? Does it have to be a substantial effect? How do we determine a substantial effect? What if it still impacts the interests of other states? And so then people, the international law scholars, they

come up with this additional concept which is reasonableness. You should be reasonable. Well that's great - that's a very clear standard. I think everybody likes reasonableness. Then people tried to go even further and say, well it's not just reasonableness - it's interest balancing. You have to actually weigh the one state's underlying policy objectives and its interest in realizing these policy objectives against the interests that the other state which might have a competing interest.

So trying to come up with something that's a little bit more tangible than just reasonableness and interest balancing, we've tried to come up with a couple of criteria which could help to determine - not criteria to be implemented by a search engine - but criteria which actually help to make sense as to whether or not, with the Article 29 Working Party or the French Data Protection Authority later says you have to implement globally, whether or not they are overstepping their bounds from the perspective of public international law.

So a first possible criteria is the risk of adverse impact in foreign states. If we think about the *Costeja* case, in particular, the chances that somebody is really going to be adversely affected by the fact that they can't find that information of a bankruptcy which happened a long time ago is really quite limited. We should look at what the purpose the delisting is, and by this I mean the underlying policy objective. You could argue that, well, it's always going to be the best achievement of the policy objective if you go for global implementation, but there are actually precedents. It seems that Google has managed to convince the European Commission in one of its competition cases that a domain-based approach is actually sufficient to give effect.

But if you compare, let's say the competition area versus the data protection area, in the competition area there are actually other thresholds — there's substantial market power - there's other, additional standards which come into play to determine what's the result that needs to be achieved in order to ensure fair competition on the market. You might not have that with protection of fundamental rights.

It also has to do a lot with what the perspective is of your attacker. Are you worried that the nosy neighbour next door is going to run a name search on you, and she's going to find some unflattering piece of information? Or are you concerned about the prospective employer, who you know, by now very well knows that search results might have been removed from their search results, but can switch to google.com to get the complete picture. Degree of harmonization - I mean, one argument that's often thrown around is when Google implement DMCA, implements copyright removal, it does this globally. Why not do the same for privacy, right? I think, I wouldn't say that copyright is one hundred percent harmonized, but I would probably accept the proposition that there's a greater degree of harmonization in the copyright sphere than there is in the privacy versus freedom of expression sphere. If there's any copyright lawyer here, you'll probably beat me up afterwards for making this statement.

The last but not least is actually to look at territorial nexi. Who is the speaker? What's his nationality? Where is he based? Where is he? Where are the servers hosted? One of the examples I like to use is to compare the case of Mr. Costeja Gonzalez against The Interview, right? If we look at the case of Mr. Costeja, we have a Spanish citizen, a piece of content information that was put forth by a Spanish newspaper on a Spanish server, all very, very strong connections to Spanish territory. Now what if, you know, Google had an establishment in North Korea, and you know, the piece of content of The Interview was there, and they said okay well, look, you have an establishment, your search results place in the context of an activity of this establishment, and so we want you to take that down. Well then we would probably come up with a different analysis. We would realize that there's a lot of people with a lot of different nationalities involved here. The movie is being produced by essentially an American company, there is no harmonization whatsoever around the world that you can talk about your supreme leader et cetera et cetera.

I'm running out of time so I'm going to finish up. The criticism - we've heard some this criticism with regard to this four-factor test. The first one is that it's subjective: states are still going to interpret in their own light, as it suits them, because in the end what they really want to do is to enforce the laws as effectively as possible. We would submit it's still better than the alternative - still better than just saying you don't have to come up with any justification, you have to take into account of any other state's interests. Another one that we hear is that it adds more complexity, you know. There's another four-factor test amongst, you know, sixty different parameters and

criteria just to decide if a right to, a request to be delisted should be granted, and now you're going to add four others? That's going to make things difficult.

That's why we actually understand the opinion of the Article 29 Working Party. They basically say, well look, if a person isn't even of local interest, if the person isn't even of public interest within the EU, chances are that they're not going to be so interesting for people in other countries. So the chances that somebody is actually going to suffer adverse impact of that search result not being available on a name search is quite small. It's probably also going to be the case that if this is local content, that there are other strong local territorial connection points, and so it's easier to send the message that it should be global by default and perhaps only restricted to local by exception.

So, in conclusion, some case by case assessment will still be necessary. Bid for global justification is justified in many instances but not all. In the case of *Google Spain*, we would submit yes. In the case of Max Mosley, we would say probably not. You know, because there is a person of international interest and people in different countries, you know, head of an international organization, they might actually have a legitimate interest and see their search results affected in a real way. And then I would actually hope, that the search engine operators resist on implementing this globally on until we can get some further clarification on this on by the courts.

CHRISTIAN WIESE SVANBERG

Attorney-at-law, Plesner

First of all I'd like to thank the organisers as well. It's a great honour and privilege to be here. It's been very interesting interventions so far and a great day. I hope to add to it.

Maybe I should add a little bit to my background in regards to what Nora has already mentioned. I initially started my career about ten years ago as a civil servant at the Danish DPA where I also served as an alternate for two years to the Article 29 Working Party. Then, I was the Chair, back in 2012, of the DAPIX Working Party which is negotiating the new draft Data Protection Regulation, which is the context that I'll be speaking from now. I have also co-authored an article that was published here by Cambridge in the Yearbook of European Legal Studies which touches upon the proposed Regulation and it has the title "*The Illusion of Harmonization*" - just so you know where I'm coming from in regards to the Regulation. As the privilege of being the last speaker in a long day of course I'll try to keep it short and to the point so let's get into it.

Just quickly I thought it might make sense to just update a little bit on the General Data Protection Regulation and what has been going on and why it is taking so long. I think one of the things that is often missed in the debate on the Regulation is that there are many reasons why this is taking some time. Initially, is it even delayed because there's no set time limit of course? What's been said is that in some ways the Council is delaying, it's postponing, it's not living up to some deadline. But there is no deadline. What is important to remember is that it took a long time to pass the current Directive. That took five years to negotiate. That was in 1995 and you only had twelve Member States. Now we have twenty eight Member States and a European Parliament that also wants to pay a big role. But even more important there are a lot of interests at stake. To give an example, back in October 2013 the European Council was supposed to discuss the Data Protection Regulation. For those of you who don't know how the Council works, at the bottom you have the DAPIX expert working party and on the top of that you have the COREPER, which is the ambassadors to the EU of all the Member States, and then you have the Council of Ministers for whatever sector you are in, so in this case it is the Justice and Home Affairs Ministers, and on top of that you have the Heads of State or Heads of Government, in what's called the European Council, and they've only discussed the Data Protection Regulation once. That was in October 2013 and what's interesting is that on the very same day as Angela Merkel was going to go to Brussels to discuss this Regulation, this exact proposal, the revelation from Snowden came out about her phone being tapped. Now you could believe that that was a coincidence, but that could have happened two months later or two months earlier. Who knows? But it happened on the very same day. Now I don't believe in coincidences of that kind. So I take that as a very illustrative example of how many and how big the

interests are that are at stake in this proposal and they are commercial, they are political and they are technological and societal and a lot of other things. I think the discussions today have demonstrated that but I think it's important to keep that in mind when you're discussing whether or not this is moving too slowly and why this is taking so long and what are they actually discussing.

Christian Wiese Svanberg, 27 March 2015, University of Cambridge

Well what's happening right now? I think it's fair to say that there has been a process in Council which is taking some time. I think they are also running out of time because I think there is a political incentive to get this done, at least in Council, within the year.

So I think that the latest development was that a few weeks ago they agreed what's called "a partial general approach" on the one-stop-shop. It was somewhat strained in the sense that it is not completely closed and there's a revision clause being put in so you can open this whole discussion up in maybe ten years time and have fun again. It was also agreed on the caveat that nothing is agreed until everything is agreed. So they're not completely agreed on this but still it's moving forward and I think that there are strong signs that they will close-up the Council part of this in June, which means that straight after that the so-called trilogue will begin. This means that the process shifts fundamentally. You go from having a large room with a lot of experts, a lot of leaks and a lot different agendas into a small room with only three stakeholders in the room being the Council presidency, the European Parliament rapporteur and the Commission's civil servant negotiating this proposal. So I think that's going to energize the process in many ways and I think it will solve some of the issues that have been created, especially in Council I have to say. The Council's process has in some ways broken down. I don't think what's happening right now is constructive on the one-stop-shop and that is going to need some fixing at some point. But then Mr Smith already touched upon that earlier.

The final timeframe - I put a question mark there because no one knows, no one can actually predict when this will happen. Some are saying that if they start in June they could do the trialogue by the end of the year. I find that fairly optimistic. That would be one of the fastest trialogue I have ever experienced and, given how big the proposal is and the stakes are high, I think that might be a bit positive. But then it may be early in 2016. That would not be completely out of the question I think. So that's probably the most likely scenario in my opinion but no one really knows.

Moving forward to the more specific point on jurisdiction. I thought that the best way to do this basically is to show what has been on the table so far regarding jurisdiction or applicable law. It's all in the same article. And actually it's one of the few articles that all the three actors, including the Council, have actually agreed some kind of common position on. So with regard to territorial scope. What the text shows is what is basically similar to the existing wording. So that's not new wording in regards to territorial application. The underlined is the Commission proposal from 2012 and now new suggested added wording. So an interesting point here is that the processor is now mentioned specifically as someone who is obligated directly by the Regulation when processing data within the Union.

Now in the second instance of the original proposal of the Commission you can see they add on some new wording and what's actually the interesting bit here is that they focus on either the offering of goods or services to data subjects in the European Union or the monitoring of their behaviour. The interesting thing here is in regards, as can be seen in the first sentence, data subjects residing in the Union and the processing is being carried out by a controller not established in the Union. Now during the negotiations in Council one of the first questions we had as we did the first round of comments on this proposal was "okay so let's say that a European citizen who resides in the Union goes to New York and is caught by a video surveillance system by a controller who's not established in the Union - that would trigger this entire Regulation then."

The second question you can ask is what is monitoring? I think the original idea from the Commission, although they were not very willing to divulge precisely what they meant by monitoring, is with regards to online tracking, information technology, cookies. Obviously that's an important issue you want to address but of course you need to make sure what this means and this goes to the heart of why it's taking a long time in Council because there are many issues like this throughout the Regulation and it's going to be difficult to define this and it's going to be one of the many issues that we have to leave to DPAs to figure out I think.

Moving forward the final part is also actually a pretty basic, already well-known text from the 1995 Directive. Doesn't really add that much. Moving to what the Parliament then suggested, they added an extra sentence to the first section of the article saying that "whether or not processing takes place in the Union". So this would mean apparently that for instance a processor who decides to, or a controller who decides to, put data somewhere else will also in regards to that data be specifically caught by the Regulation. That makes sense in a certain way.

The bold here, is additional wording from the Parliament - what they thought was important to add. They've added "or processor" so again, a processor is now specifically targeted as a subject to regulate by the law. Obviously that also adds new questions and layers of complexity to work with. What will this actually mean for someone like Google? I'll come to that at the end. Also an important issue is whether or not a commercial transaction takes place. But again they're keeping the idea of monitoring data subjects in the text. Actually, the Council is doing something very similar. Here is their proposal. In order to address the issue that I mentioned earlier about video surveillance going on in New York they narrow the provision to only take into account the monitoring that is covering behaviour that takes place within the European Union. So this would still presumably catch a tracking cookie being placed or following someone within the European Union but not if you are exposed to some sort of surveillance while on holiday on the Maldives. So that makes sense. Again maintaining the traditional public international law jurisdictional approach.

So what will this all lead to? Well, at the end of the day, I think it's fairly certain that there will be probably a large degree of extraterritoriality. That's plain to see. All three co-legislators, all the three institutions, agree that the rules

should apply in third countries. This raises a number of questions of course. The first of all is what is "monitoring" as I already mentioned, which is a separate issue. You can argue that for a long time and again the DPAs will have a lot of work cut out for them trying to figure out whether or not this rule has been triggered or not and if it has, how they enforce those rules. Coming from the Ministry of Justice, being a lawyer who cares about how you draft rules, I have to say that making rules is one thing, but you always want to make rules you can actually enforce in reality, for many reasons. Just as I am not a big fan of the title of the "right to be forgotten", because I think it creates false expectations. I think the same is the case if you're setting up rules that you claim apply to what is going on in a third country and not providing tools or realistic options for the authorities to enforce those rules. So I think that's going to be a central issue, that is probably not going to be solved by the legislator but more by the facts on the ground. I think it will create unrealistic expectations and you can also ask what will a third country think about the EU extending its competence in this way. Some will argue well the US for one is already doing this but, well, the world is bigger than just the US and I think the EU needs to consider carefully whether it is a suitable way to go to impose their rules on what's going on in third countries. But I'm afraid that then no one is going to be listening to me in this regard. I think it is definitely going to happen no matter what I say here today. What does this mean for the *Google Spain* precedent? Given the fact that that the court has said pretty clearly that they consider Google to be a data controller I don't think that there can be much doubt that these rules will obviously be triggered in regards to almost anything that someone, Google or any other search engine, will be doing because they will either be a data controller or a data processor, most likely a data controller given the precedent. Obviously, as long as you are using the same terms as have been laid out by the Court in the verdict there's no reason to assume that the law would be different. So going forward I think this is still going to be an issue and the place to solve that would be in the definition and the elaboration of the right to be forgotten in the actual Regulation and that is yet to be closed.

> *I often think when I hear discussions about this verdict that there is, what you might call a degree of cognitive dissonance.*

So that's all I want to say.

Let me just leave with one observation I made listening to some of the earlier interventions during the day. I often think when I hear discussions about this verdict that there is, what you might call a degree of cognitive dissonance. On the one hand, the argument is that it is absolutely crucial that data be removed from search engines, from Google. I think that the wording was in the *Costeja* case that the problem was Google. It was not the initial publication that was the issue. It was crucial that he went to Google and had the data removed because that's where people found the data. But then, on the other hand, sometimes even the same people in the next sentence can pivot and say "well when it comes to the discussion of freedom of speech and possibly censorship, well, Google is not really that important." "It's not where we find our information necessarily". "It's only part of our information resource." Google surely has to be important in both respects? I think it's important to recognize that fact and also recognize that the basic tension is that on the one hand you have a societal value which is freedom of speech and then you have a more perhaps personal value. So in each specific instance, there will always be a tendency to lean towards recognizing the individual's right to have something deleted and no one's really advocating the sort of societal side of that issue. I think that's a big tension right now in the debate and that's an issue. Where this can end up is going to be very interesting to see going forward. I don't have the answer.

FLOOR DISCUSSION, QUESTIONS AND RESPONSES

Question: A delegate commented that territoriality had become an elephant in the room for data protection. He asked how this situation came to develop.

Professor Caspar responded that we are living in a constitutional state and where things are not forbidden they are allowed. We need complex and effective structures to protect the rights of individuals. We could not afford to wait another four years for the Regulation, given the time for negotiation and implementation. This was too long a period in his opinion.

Mr Van Alsenoy noted that Google has framed the territoriality as such because Google operates on a global scale and it is logical that they will not apply all laws across the board. They have tried to impose on cyberspace a structure that works and makes sense so he would not necessarily fault them for doing so. There was a long accepted practice by Google before Google Spain where they have taken a more filtering approach, rather than a domain-based approach. The possibilities or circumvention are very high even if you opt for more strictly origin-based filtering. He gave the example of cheap and fast methods to circumvent origin-based restrictions on access to television content online.

Question: A delegate gave the example of teacher rating websites which came up in German jurisprudence in the Spichmich case. He asked the panel to suppose that the leading rating website in the future was based in a non-EU jurisdiction that had very strong freedom of expression but had moderators in schools within the EU to ensures that its rating procedures were not circumvented. Under the proposed Regulation, the use of equipment test drops away. He asked whether the presence of monitors constituted stable arrangements or an establishment because it is appointing moderators for a period of time. Secondly, on monitoring of behaviour, drawing up a list of teachers and asking for ratings does appear to be monitoring of behaviour on a literal interpretation of the words. He asked first whether the panel saw the rules applying under the Regulation in that situation and how the panel saw enforcement actually operating, if at all.

Professor Caspar answered on the applicability of the Regulation that a website addressed to Germany would be within the Regulation. The second question was how to enforce the law in the US. It was a very hard question because Data Protection Authorities can only enforce if there is a data controller that answers your questions and comes to Europe. The big internet players can be controlled in a much better way because there are here and can be controlled much easier.

Mr Van Alsenoy answered that whether moderators were an establishment might depend on whether advertising was sold. The use of the concept of monitoring was supposed to be a more elegant solution that relying on use of equipment but the term monitoring shifts us too much towards the tracking perspective. Perhaps we need to look at regular processing of data about, or frequent collection of information regarding, EU data subjects. On the enforcement question, you need physical present here. In the Yahoo! case where an auction website was selling Nazi paraphernalia and the French court held that so long as it was accessible in French territory it was a violation of French law and Yahoo had to take action to prevent it. That was further litigated in the United States.[1] They wanted declarative relief that the French order was not enforceable in the US. This was not resolved because the plaintiffs were not seeking enforcement but Yahoo! ultimately complied with the French order. For a multinational company the appearance of compliance with the law was important for consumer trust and public relations.

Mr Svanberg answered that the new territorial application would also be triggered by a processor directly so a monitor might trigger the Regulation. Criminal responsibility could also potentially be triggered by some sort of collusion or accessory to the crime. This is all going to be criminally enforceable rules and fines. Accessory liability, though far-fetched, might be an option.

Question: A delegate asked whether ISP enforcement could be a solution to the problems discussed.

Mr Van Alsenoy answered that we not want a firewall around Europe. There are more proportionate responses available. It can be in the interest of advertising business to establish in the EU. ISP enforcement would be a bad idea. He said he was not a big fan of the strategy.

HANDOUT: DATA PROTECTION & THE INTERNET AFTER GOOGLE SPAIN

DR. DAVID ERDOS
(UNIVERSITY OF CAMBRIDGE)

NOTE ON EEA DATA PROTECTION AUTHORITY SURVEY 2013

- This survey was run between **March and the end of July 2013,** i.e. before the handing down of *Google Spain.*
- It achieved a response rate of **around 80% of national European Economic Area DPAs**, together with a further **six** authorities operating at the **sub-national** level.
- The survey addressed a wide range of issues connected to the interface between Data Protection and the Open Society, with a special focus on online media.

Questions on Legal Interpretative Stance as Regards Online Media

DPAs were asked to assess a number of hypothetical scenarios, which were designed to be linked seven distinct types of new online media

1. **Newspaper archive -** *"A searchable online newspaper archive publishes a newspaper story originally published a decade ago concerning a living individual."*
2. **Individual blogger -** *"In his spare time, an individual publishes a blog that discusses and disseminates gossip about various celebrities. It is freely available on the Internet and visited by several hundred people a week."*
3. **Individual on social networking site -** *"A member of a Social Networking Site (SNS), the membership of which is generally open to individuals worldwide, 'tags' a photo of an identified individual and makes an informed decision to make this freely available to all members of the site."*
4. **Social networking site -** *"The Social Networking Site (SNS) is contacted directly by the same identified individual as above [i.e. the data subject mentioned in scenario 3 above] who claims that the Site itself is a Data Controller in relation to this processing."*
5. **Internet rating website -** *"A company establishes a website freely available on the Internet allowing individuals to 'rate' and add comments about their teachers."*
6. **Internet search engine -** *"A company provides a service allowing people to search the information sources of the public Internet (including on identified individuals) through a web-based search engine."*
7. **Street mapping service -** *"A street mapping service produces maps with street-level photographic images including pictures of individuals, motor vehicles and homes."*

In each case they were invited to indicate which one of the following statements was considered correct:

a. Data protection does not apply.
b. Data protection applies, but the activity in question must benefit from all the special purposes derogations and exemptions for journalism, art and literature envisaged in Article 9 of Directive 95/46/EC.
c. The general provisions of data protection apply, but must be interpreted with regard for other fundamental rights including freedom of expression.
d. The general provisions of data protection law apply in full.

(As an alternative, DPAs were able to provide a free-text specification of the relationship between Data Protection and the activity in question. Some provided additional text for further elaboration.)

Implementation of Data Protection

- DPAs were asked to indicate whether, in relation a processing activity connected to publication, they had taken **enforcement action against** (*inter alia*) the **same seven online media actors** listed above, since the Data Protection Directive 95/46 had been transposed.
- If they had, they were invited to indicate in very broad terms in what context enforcement action had taken place.
- In addition, DPAs were asked to specify their **annual budget** dedicated to data protection issues. (Where part of their budget was also dedicated to another issue such as Freedom of Information, they were invited to provide an estimate of the part of the budget allocated to data protection).

LIST OF PARTICIPANTS

Julia Apostle, Twitter

Jef Ausloos, University of Leuven – ICRI/CIR-iMinds

David Barker, Pinsent Masons LLP

Kim Barrington, BBC

Ben Beabey, News UK

Paul Bernal, UEA Law School

Jane Berry, Norton Rose Fulbright LLP

Reuben Binns, University of Southampton

Sarah Branthwaite, Wiggin LLP

Ana Breitinger, Queen Mary, University of London

Sally Broughton Micova, LSE Media Policy Project

Genevieve Burley, University of Cambridge

Ian Burton, Google

Oliver Butler, University of Cambridge

Caroline Calomme, University of Oxford

Giovanna Carloni, Queen Mary, University of London

Johannes Caspar, Hamburg Commissioner for Data Protection and FOI

MacKenzie Common, University of Cambridge

Andrew Cormack, Jisc/Queen Mary, University of London

Charles Crisp. University of East Anglia

Angela Daly, Swinburne Institute for Social Research

Richard Danbury, University of Cambridge

Willem Debucklaere, Belgium Data Protection Authority

Nigel Dexter, Department for Education

Janine Discher, University of Cambridge

David Erdos, University of Cambridge

Lisa Fleisher, The Wall Street Journal

Andrew Gallie, Veale Wasbrough Vizards

Jodie Ginsburg, Censorship

Vesela Gladicheva, MLex

Ann Kristin Glenster, University of Cambridge

Dorota Glowacka, Helsinki Foundation for Human Rights

Matthias Goetz, University of Cambridge

James Henderson, Hunton and Williams

Meryem Horasan, University of Strathclyde

Victoria Hordern, Hogan Lovells

Michael Hopp, Plesner

Kirsty Hughes, University of Cambridge

Hannah Jackson, Hogan Lovells

Victoria Jolliffe, 5RB Chambers

Penelope Jones

Irini Katsirea, Middlesex University Law School

Donal Kerr

Harry Kinmonth, RPC

Rebekah Larsen, University of Cambridge

James Leaton Gray, BBC

Orla Lynskey, LSE

Mac Macmillan, Hogan Lovells

Paul Magrath, ICLR

William Malcolm, Google

Alex Marzec, 5RB Chambers

Athalie Matthews, Bindmans LLP

Jonathan McCully, Media Legal Defence Initiative

Felicity McMahon, 5RB Chambers

Lucy Middleton, Addleshaw Goddard

Richard Mortier, CU Computer Laboratory

Michael Moss, Northumbria University

Lukas Mrazik, Queen Mary, University of London

John Naughton, CRASSH/Wolfson College, University of Cambridge

Nora Ni Loideain, University of Cambridge

John O'Brien, Hogan Lovells

Eoin O'Dell, Trinity College Dublin

Kieron O'Hara, University of Southampton

Mike O'Neill, Baycloud Systems

Stephanie Palmer, University of Cambridge

Steve Peers, University of Essex

Miquel Peguera-Poch, Universitat Oberta de Catalunya

Gill Phillips, Guardian News and Media

Andelka Phillips, University of Oxford

Chris Pounder, Amberhawk

Julia Powles, University of Cambridge

Artemi Rallo Lombarte, Jaume I University

Renate Samson, Big Brother Watch

Diana Sancho, University of Leicester

Julian Santos, 5RB Chambers

Alice Schneider, University of Oxford

Fatos Selita, Emerging Law

Jeff Skopek, University of Cambridge

David Smith, Information Commissioner's Office

Ilke Soysal, University of Strathclyde

Linda Stewart, The National Archives

Clive Thorne, Wedlake Bell LLP

Laura Tielemans, Vrije Universiteit Brussels

Hugh Tomlinson QC, Matrix Chambers

Judith Townend, Institute of Advanced Legal Studies

Eduardo Ustaran, Hogan Lovells

Brendan Van Alsenoy, ICRI/CIR, KU Leuven – iMinds

Alinda Vermeer, Media Legal Defence Initiative

Simon Weidler, Queen Mary, University of London

Andrew Wheelhouse, Bates Well Braithwaite

Christian Wiese Svanberg, Plesner

Ralph Wilkinson, Norton Rose Fulbright LLP

Estelle Wolfers, University of Cambridge

Nixin Xie, Queen Mary, University of London

Todor Yotov, Privacy Shelter

Ben Zevenbergen, Oxford Internet Institute

Nicolo Zingales, Tilburg University