European Regulatory Interpretation of the Interface between Data Protection and Journalistic Freedom: An Incomplete and Imperfect Balancing Act?

David Erdos[1]

Abstract:

Directive 95/46 required European Economic Area Member States to ensure a careful balancing between the inherently conflicting values of data protection and journalistic freedom of expression. Unfortunately, however, this was often not achieved during the transposition of the Directive into local law. At the same time, both Directive 95/46 and the Art. 7 of the EU Charter mandated Member States to set up supervisory Data Protection Authorities (DPAs) which in practice dominate the data protection landscape. In light of this, EEA DPAs were surveyed on their understanding of the right to subject access and the practice of undercover political journalism, with the responses then compared to provisions in local data protection law. The results demonstrated that DPAs do seek a balance in this area even against contrary statute. Nevertheless, the balancing achieved often remains incomplete, normatively contestable, opaque and precarious. It is argued that, during the implementation of the General Data Protection Regulation, these challenges must be tackled through a combination of both legislative and regulatory action.

Keywords: Data protection, Direct effect, Directive 95/46; European harmonization, EU Charter, freedom of expression, General Data Protection Regulation; media freedom, media regulation, privacy, subject access, undercover journalism.

[1] University Lecturer in Law and the Open Society, Faculty of Law and WYNG Fellow in Law, Trinity Hall, University of Cambridge. I would like to thank both the Data Protection Authorities and the many individuals who assisted in the research presented here, as well as the British Academy who supported it. I particularly thank Michèle Finck who provided invaluable administrative assistance as regards the survey, Richard Danbury who commented on a previous version of this manuscript and Rebekah Larsen who assisted with some last minute checks. Any errors remain my own.

Through the "exercise by occupation of the right to free expression",[2] traditional journalism disseminates a wide variety of information to a broad and unrestricted public. In contrast, European data protection has as its central purpose the safeguarding of information relating to natural persons so as to ensure that their privacy and related rights are not undermined.[3] Inevitably, therefore, data protection and journalistic freedom of expression coexist within a state of great tension. This tension was recognised in article 9 of the EU Data Protection Directive 95/46 which mandated that European Economic Area (EEA) Member States[4] set out a "balance between fundamental rights" in this area, whilst nevertheless still ensuring that an "equivalent" standard of data protection through Europe was attained.[5] Since 2009, these stipulations have been bolstered by the recognition of both data protection and freedom of expression as fundamental rights within the *EU Charter*,[6] together with protection of the former also within the EU treaties themselves.[7] Unfortunately, however, this vision of careful balancing has often not been achieved within Member State local statutory law.[8]

Alongside these substantive stipulations, both the *EU Charter* and Directive 95/46 mandate the establishment of Data Protection Authorities (DPAs) in each Member State with wide-ranging supervisory responsibilities. In practice, these agencies are seen as "the guardian[s] of data protection"[9] and, therefore, play the leading role in this area. In light of the both the practical

[2] G. Robinson, *People Against the Press: An Enquiry into the Press Council* (London: Quartet Books, 1983), p. 3.
[3] See Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) (ETS 108), art. 1; Directive 95/46, art 1.1.
[4] Directive 95/46 binds not just the EU but also Iceland, Liechtenstein and Norway under the Agreement on the European Economic Area ([1994] OJ L 1/7). The precise relationship between these States and the data protection provisions in the EU Charter and Treaties remains much more complex. Following the results of a referendum on 24 June 2016, the UK Government is now committed to the UK (together with the UK's intra-EU overseas territory of Gibraltar) leaving the EU. The UK Government's position on continued membership of the EEA remains more ambiguous. For now, however, the UK remains a full member of the EU, as it was when the data presented in this article was collated.
[5] Directive 95/46, recitals 11 and 8.
[6] EU Charter of Fundamental Rights, arts 8 and 11.
[7] TFEU, art 16 (1).
[8] D. Erdos, "European Union Data Protection Law and Media Expression: Fundamentally Off-Balance" (2016) 15 *I. C. L. Q.* 139.
[9] P. Blume and C. Svanberg, "The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Private/Public Divide and the Bureaucratic Apparatus" (2013) 15 *C. Y. E. L. S.* 27, 40.

centrality of the DPAs and the importance of the tension between data protection and journalistic freedom, this article explores how these authorities approach their interpretative stance within a legal context which is "rife with inconsistencies".[10] A survey of EEA DPAs was undertaken in 2013 securing the participation of over 75% of these authorities at national level together with six sub-national bodies. This survey probed DPAs by, firstly, asking them about relationship between journalism and the right of subject access and, secondly, by requesting them to assess the general data protection position of a hypothetical journalist engaging an undercover political investigation. Over the same period, the relevant local statutory provisions were also analysed and coded.

The results indicate that, although there is a relationship between the stringency of local statutory provisions and DPAs' interpretative stance, many agencies do seek to balance journalistic freedom alongside data protection even against the express wording of local statute. Nevertheless, as will be elucidated, this balancing remains incomplete and, given its contestable, opaque and precarious nature, in any case imperfect. Many (although not all) of these limitations arise from the failure of national legislators to adopt legible and balanced statutory provisions here. Article 85 (2) of the now finalized General Data Protection Regulation, which will replace Directive 95/46 in May 2018, essentially repeats this existing instruction.[11] It is, therefore, essential that during its implementation into local law, Member States diligently fulfil this task. At the same time, adoption of the Regulation will provide DPAs themselves with a renewed opportunity to ensure a more coherent regulatory approach including through the drawing up of a formal Recommendation by the new European Data Protection Board.

The rest of this article is structured as follows. The next two sections set out the legal context and both the questions posed and methodology adopted in this research. The following two sections present the research results, whilst the following one systematically compares DPA interpretative approaches with the provisions found in local statutes. The penultimate section

[10] P. Keller, *European and International Media Law* (Oxford: OUP 2011), p. 339.
[11] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.

provides a normative assessment of these results, whilst the last closes with some brief conclusions and suggestions for reform.

Legal Context

The Default Data Protection Framework

Drawing inspiration[12] from the 1981 Council of Europe Data Protection Convention which remains in force, the European Union data protection regime centred on framework Directive 95/46 occupies a critical position within EU fundamental rights and has "become the central field for the development of privacy law and policy".[13] Its material scope, purpose and standards are extremely wide-ranging. At least within the private sector,[14] it applies to any "processing of personal data wholly or partly by automatic means" or even in certain structured, manual filing systems.[15] All the key terms are defined broadly. "[P]ersonal data" refers to "any information relating to an identified or identifiable natural person ('data subject')", whilst "processing … by automatic means" includes "any operation" including collection, retrieval, consultation, dissemination and erasure.[16] Meanwhile, its object is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy", at the same time prohibiting restrictions on the free flow of personal data between European Economic Area (EEA) jurisdictions for reasons connected with such protection.[17] Reflecting these multifaceted purposes, data "controllers" – that is anyone "who alone or jointly with others determines the purposes and means of the processing of personal data"[18] – must by default ensure that their processing complies with a set of data principles centred on fairness and legitimacy, detailed rules ensuring the transparency of processing and generally

[12] Directive 95/46, recital 11.
[13] P. Keller, *European and International Media Law* (2011), p. 331.
[14] Subject to an extremely narrow "purely personal or household" exemption for individuals (Directive 95/46, art 3.2).
[15] Directive 95/46, art 3.1.
[16] Ibid, art 2 (d).
[17] Ibid, art 1.
[18] Ibid, art 2 (d).

prohibiting the processing of sensitive data absent waiver from the data subject and finally a range of data security and other control mechanisms designed to ensure genuine discipline in data processing. Turning to the system of supervision, in addition to providing a judicial remedy, Member States must establish one or more independent DPAs endowed with wide-ranging powers of investigation and intervention and required to monitor the law's application and hear claims from data subjects. Representatives of the DPAs must also cooperate in a pan-European Article 29 Working Party which has a duty to promote "uniform application" of Directive 95/46 across the EEA, notably through issuing official Opinions and Recommendations.[19] In practice, these statutory bodies play the leading role in both the shaping and applying of data protection within the EU. Indeed, Blume and Svanberg go as far as to state that "[t]he credo is that without the agency, there is no data protection".[20]

Although Directive 95/46 was adopted under the EU's general power to regulate the internal market, from 2000 a right to data protection was set out within the new *EU Charter of Fundamental Rights.* This provision's enumerated core included the data subject's "right of access to data which has been collected concerning him or her and the right to have it rectified". The Charter also stressed the crucial supervisory role of DPAs stating that "[c]ompliance with these rules shall be subject to control by an independent authority".[21] In December 2009, the Treaty of Lisbon granted the *EU Charter* the same legal status as the EU Treaties.[22] Uniquely amongst these enumerated Charter rights, it also amended the treaties themselves so as to separately provide that "[e]veryone has the right to the protection of personal data concerning them".[23] A new and specific legal base for enacting data protection law was also established.[24] Following on from this, in 2012, the

[19] Established under art 29 of Directive 95/46, this group comprises a DPA representative from each of the EU Member States together with two pan-EU members, namely, the European Data Protection Supervisor and a (non-voting) representative of the European Commission. The non-EU EEA DPAs participate in the Working Party as observers.
[20] P. Blume and C. Svanberg, "The Proposed Data Protection Regulation", 40.
[21] *EU Charter*, art 8.
[22] TEU, art 6 (1).
[23] TFEU, art 16 (1).
[24] TFEU, art 16 (2).

European Commission proposed replacing Directive 95/46 with a new General Data Protection Regulation.[25]

Traditional Journalism and Data Protection

Traditional journalism (hereinafter journalism) refers to the remunerated production and periodic institutional distribution of information and opinions to a large and indeterminate number of people on the basis of their real or purported quality of public interest and link to contemporary societal developments.[26] Such activity not only leads to "the collection and storage of huge amounts of personal information"[27] but it has been argued that, at least within the private sector, "it is the media … which is capable of inflicting the gravest damage on the individual"[28] as a result of personal information processing. In other words, journalism not only falls within the scope of data protection, but also has the potential to severely undermine its central safeguarding purpose. At the same time, full application of data protection's strictures to journalism would severely curtail its freedom and "could devastate the media".[29] This is particularly problematic since journalism constitutes a central instance of the exercise of the right to freedom of expression.

Although Directive 95/46 did recognize this fundamental tension between journalism and data protection, it left much of the detail of its resolution to the local level. In sum, article 9 of the Directive provided that, as regards processing carried out for journalistic purposes (or the purpose of artistic or literary expression), Member States had to provide derogations from any of its substantive

[25] COM (2012) 11 final.
[26] See M. Shudson, *The Sociology of News* (New York: Norton, 2003), p. 11.
[27] P. Keller, *European and international media law* (2011), p. 331.
[28] Great Britain, House of Lords, Select Committee on the European Communities, *20th Report: Protection of Personal Data* (London: HMSO 1993), 39.
[29] S. Rasiah and D. Newell, "Data Protection and Press Freedom" (1997/98) 3 *Yearbook of Media and Entertainment Law* 232.

and most of its procedural provisions[30] but "only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression". Recital 37 stressed that the derogations adopted should be those "necessary for the purpose of balance between fundamental rights",[31] whilst recital 8 set out the more general and overarching requirement that the level of data protection "must be equivalent in all Member States". These strictures were emphasized by the Court of Justice of the European Union (CJEU) in *Satamedia* (2008) which found that even in the journalistic area "the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data … must apply only in so far as is *strictly* necessary".[32] However, the Directive's vision of an equivalent and proportionate legal framework in this area was far from achieved during its transposition into Member State law. To the contrary, the most extreme diversity of treatment is apparent in local statutory data protection law. In sum, most northern European jurisdictions grant media expression an overwhelming priority within their law, with some even entirely disapplying all substantive data protection provisions here.[33] Meanwhile, most Latin and eastern European countries accord a similar priority to data protection, with a number[34] granting the media no derogations at all. Almost every permutation between these extremes is also apparent within one or more of the EEA jurisdictions. This confusing reality has been comprehensively set out and analysed by the author in a previously published article[35] which may be consulted for any statutory references not specifically cited here.

The presence of open-textured human rights within constitutional or otherwise foundational national and European instruments adds a further layer to what is already an intricate legal

[30] Article 9 excluded the possibility of derogations from the right to a judicial remedy (art 22), the right to compensation for damage arising from legal fault (art 23) and from the requirement to adopt suitable measures and sanctions to ensure the Directive's full implementation (art 24).
[31] It also specified that the derogations should not "lead Member States to lay down exemptions from the measures to ensure security of processing" and "at least the supervisory authority responsible for this sector should also be provided with certain ex-post power e.g. to publish a regular report or to refer matters to the judicial authorities."
[32] C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, EU:C:2008:727 at [56] (emphasis added).
[33] Namely, Finland, Norway, Sweden and, as regards the Press, also Germany.
[34] Namely, Spain, the Czech Republic and Croatia.
[35] D. Erdos, "European Union Data Protection Law and Media Expression".

landscape. Not only the *European Convention on Human Rights (ECHR)*[36] and the *EU Charter*[37] but also the great majority of Member States' constitutions grant some form of protection both to freedom of expression and to privacy. Moreover, the constitutions of just under half of the Member States and now also the *EU Charter*[38] itself also explicitly include a right to data protection.[39] The Article 29 Working Party's first ever formal Recommendation also explored (albeit in only six full pages) the topic of *Data Protection Law and the Media*. Although produced before adoption of the *EU Charter*, it gave emphasis to the broader human rights background. Thus, on the one hand it stated:

> In most cases, independently of any express derogation that may exist, data protection legislation does not apply fully to the media because of the special constitutional status of the rules on freedom of expression and freedom of the press. These rules place a de facto limit on the application of substantive data protection provisions or at least their effective enforcement.[40]

On the other, it also stressed that "[t]he right to privacy is similarly guaranteed by article 8 of the ECHR. Data protection comes within the scope of the protection of private life guaranteed under this article".[41] As hinted at in the first quotation from the Working Party, in many cases constitutional (or otherwise foundational) provisions in Europe operate as a vertical shield against inconsistent State laws (or other action) but not horizontally against the activities of other private parties.[42] Nevertheless, from 2009, the Lisbon Treaty added a further important crease to this complexity. As noted above, in addition to according the *EU Charter* the same legal status as the EU

---

[36] *European Convention on Human Rights*, arts 10 and 8.
[37] *Charter of Fundamental Rights of the European Union*, arts 11 and 7.
[38] Ibid, art 8.
[39] See discussion in J. Cannataci and J. Misfud-Bonnici, "Data Protection comes of Age: The Data Protection Clauses in the European Constitutional Treaty" (2005) 14 *Information and Communications Technology Law* 8.
[40] EU, Article 29 Working Party (1997), p. 6.
[41] EU, Article 29 Working Party (1997), p. 4. Given the huge breath and innovative content of data protection, such a statement was clearly controversial.
[42] Nevertheless, a failure to appropriately protect individuals against private action can result in the finding of a violation against the State. See e.g. *Von Hannover v Germany* (2005) 40 EHRR 1.

treaties, Lisbon also entrenched the right to data protection in the treaties themselves. It has been cogently argued that this latter provision may have not only vertical but also direct, horizontal effect.[43] If true, then this right could even be invoked against the media's gathering and use of personal data.

Questions and Methodology

Given the pan-European legal context above, how should the data protection responsibilities applicable to journalism be construed? In light of their critical role within the data protection landscape, it was decided to pose this dilemma to the statutory DPAs operating across the EEA and then systematically compare these responses to stipulations found within formal statutory data protection law. A survey was sent to both national and sub-national[44] EEA DPAs, initially in March 2013, with replies being received until the end of July 2013.[45] Relevant replies were received from 24 (over 75 per cent) of national DPAs together with six authorities operating at the sub-national level. At the same time, a detailed coding of local statutory data protection law was also completed.

Turning to the specific questions put to the DPAs, it was recognised that given the wide range of duties which data protection could potentially impose on the media, it would be impracticable to probe these agencies in detail on all of its aspects. Instead, two very differently focused questions were formulated. The first sought to gauge DPAs' specific understanding of journalistic responsibilities vis-à-vis one highly innovative aspect of data protection, namely the right of subject

[43] O. Lynskey, "From Market-Making tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis" in S. Gutwirth, R. Leenes, P. de Hert and Y. Poullet. (eds.), *European Data Protection: Coming of Age* (Dortrecht: Springer, 2013) at p. 77 (citing opinion also of the then European Data Protection Supervisor Peter Hustinx).

[44] Sub-national DPAs have been established in Spain and Germany as well as in Gibraltar, a British Overseas Territory within the EEA with a data protection scheme which is nevertheless separate from that of the mainland UK.

[45] Given that the survey as a whole explored not just journalism but a range of matters related to data protection and openness, the survey was not sent to the specialist media regulators which in Lithuania and Denmark exercise limited regulatory powers over the media even in relation to data protection. Nevertheless, the Lithuanian DPA made clear that its responses here had completed in cooperation with the Inspector of Journalist Ethics. The Danish DPA did not participate in the survey.

access. By default, this right mandates that, on request from a data subject, controllers ensure a comprehensive retrospective transparency of their processing by providing data subjects with access to all data relating to them.[46] In contrast, the second presented DPAs with a hypothetical scenario based on the ubiquitous, but sometimes controversial, practice of undercover political journalism and asked them to assess its general legality vis-à-vis the data protection framework as a whole.

As regards both of these questions, DPAs were presented with five standardized, categorical responses (labelled hereinafter (a) to (e)). As far as possible, these were designed to coalesce, albeit in a necessarily simplified form, with the coding then in progress of the local statutory law in each Member State. The responses were also constructed so as to range from the logically most stringent possibility (full/100% application of default data protection) through to the least (no/0% application of the same). Therefore, it was possible to array these responses along a 0-1 scale such that (a) was equal to 1, (b) to 0.75, (c) to 0.5, (d) to 0.25 and (e) to 0. As will be seen, such a translation aids systematic comparison especially between the statutory and DPA interpretative dimensions. Finally, in light of the complex legal issues raised by the second question, DPAs were alternatively invited to provide an individually tailored free-text answer if they so wished.

Subject Access and Journalism

DPA Survey Question and Responses

The first question asked DPAs whether an individual who was the subject of a journalistic investigation by a media entity had the right to access the data held by that entity in the context of the investigation.[47] The five standardized responses set out in relation to this question were as follows:

[46] Directive 95/46, art 12.

[47] The question cited in brackets art 14 of Directive 95/45 which, although concerned with the data subject's right to participate in processing concerning them, does not provide detail on the provisions concerning

a. Yes, the same legal provisions apply here as in relation to other data controllers.

b. Yes, the individual could have access to the data (with the exception of information relating to journalist sources, which would be protected from such disclosure).

c. A modified procedure applies whereby the Data Protection Authority accesses the data on behalf of the data subject.

d. Yes, in principle but in addition to the non-disclosure of journalist sources, such rights may be outweighed by the media entity's right to freedom of expression (and related rights).

e. No.

Twenty-nine standardized responses were received here, which are summarized in Chart One and set out at an individual DPA level in Table One later on in this article. As can be seen, one DPA (3% of the total) indicated, albeit with certain supplementary caveats,[48] that subject access would apply without distinction as with other data controllers (category a/1). Eleven DPAs (38%) stated that general access rights would apply to all but a journalist's sources (category b/0.75). Two DPAs (7%) held that in journalistic cases subject access would be secured vicariously through the DPA itself (category c/0.5). Ten DPAs (34%) held that, whilst an individual had a right to make a subject access request, it might nevertheless be outweighed by the media's rights including to freedom of expression (category bd/0.25). Finally, five DPAs (17%) held that subject access rights would not apply in the media context (category e/0). In addition, one DPA set out a non-standardized free-text answer which appeared to sit somewhere between categories a/0 and b/0.25.[49]

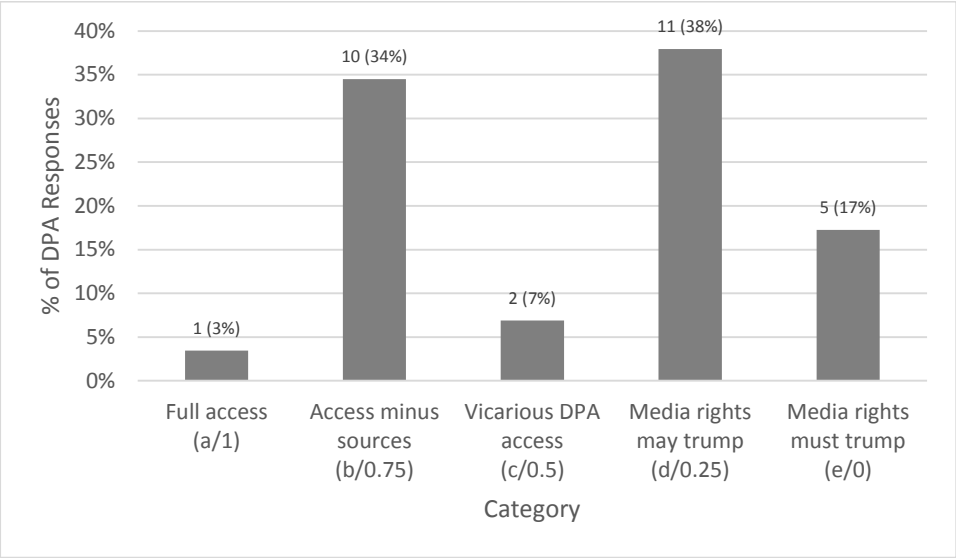
---

subject access. The clearly defined nature of the question itself and the potential responses to it ensured that there was no confusion as to the focus of the inquiry.

[48] In sum, the Cypriot DPA appended supplementary text which stated that "[w]hen planning to publish an exposé it is a common practice for journalists to ask the persons involved to comment on it prior to publication. We have had no cases of access to media insofar. In Cyprus the Journalists Code of Ethics is not binding by virtue of Law. The Code provides inter alia that a journalist is not obliged to reveal his sources." This DPA also added a general caveat to all of its answers in the survey that "[e]ach case is examined on a case by case basis taking into account its own merits and particularities."

[49] In sum, the UK DPA answered "[i]n principle yes, the individual has the right to make a subject access request under section 7 of the DPA [Data Protection Act]. However, in practice the organisation is likely to be

Chart One: Subject Access and Journalism – EEA DPA Standardized Responses (n = 29)



B. Position in Statutory Law

Drawing on a more fine-grained and detailed analysis presented elsewhere,[50] it was possible to array the statutory data protection law in each of the relevant DPA jurisdictions along a similar spectrum to the above. Such a coding indicated that statutory law in seven of the DPA jurisdictions (23% of the total) provided no journalistic derogation from subject access (category a/1). In three DPA jurisdictions (10%) the law generally mandated full application of the default subject access right but nevertheless shields from disclosure data regarding the sources of journalistic information (category b/0.75).[51] In two further jurisdictions the law provided for vicarious access by the DPA in media cases (category c/0.0.5). In nine DPA jurisdictions (30%) the law required some kind of balancing between the individual's right to subject access and journalistic freedom of expression (category d/0.25), albeit with very different weights often being given to these two legal values. In

able to apply the special purposes exemption in order to refuse to supply the requested information in response to the request".

[50] D. Erdos, "European Union Data Protection Law and Media Expression", pp. 161-163.

[51] In Bulgaria such shielding is clearly restricted to sources who are natural persons. In contrast, the Hungarian and Italian provisions are more wide-ranging and would, therefore, also protect organisational sources.

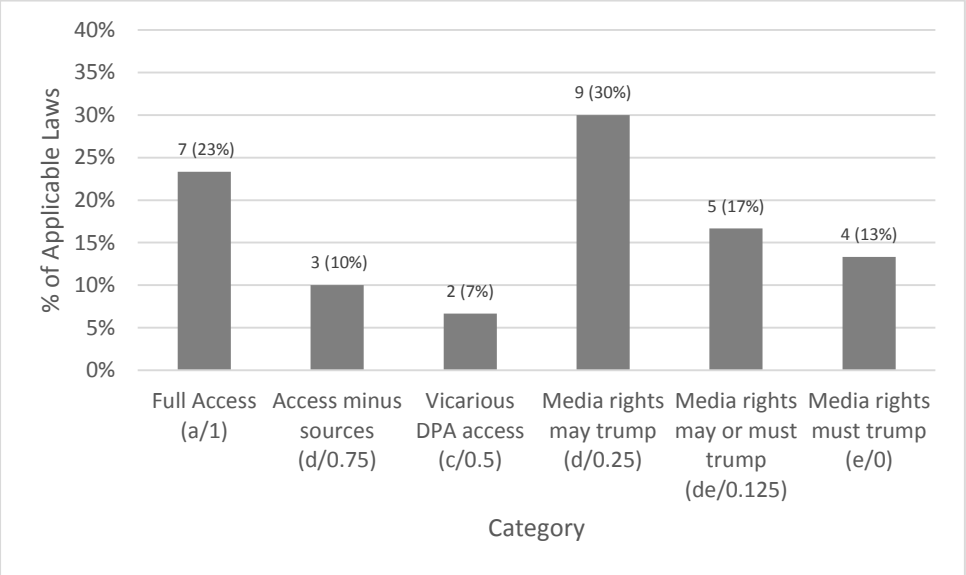
four DPA jurisdictions (13%) the statutory law simply exempted journalistic processing completely from compliance with the rules on subject access (category e/0). More complexity was apparent in the five German DPA jurisdictions which responded to the survey (17%). In each of these jurisdictions, the law applicable to certain broadcasters required journalists to apply an, albeit relatively media-friendly, balancing test between subject access and freedom of expression (category b/0.25).[52] On the other hand, the Press benefit from a complete legal immunity here (category e/0),[53] with normative guidance being left entirely to self-regulation.[54] Given the potential applicability of either of these regimes within the journalistic sector, these jurisdictions were allocated a coding of 0.125 which is midway between category d/0.25 and category e/0. These results are summarized in Chart Two below and set out at individual DPA level in Table One later in this article.

[52] All these provisions are modelled on the German Interstate Treaty on Broadcasting and Telemedia, art 47 (2). The specific statutory provisions are as follows: Germany, Federal Data Protection Act, sec 41 (2)-(4); Landesmediengesetz (LMG) Rheinland-Pfalz, sec 12; Staatsvertrag über das Medienrecht in Hamburg und Schleswig-Holstein (Medienstaatsvertrag HSH); Rundfunkgesetz für das Land Mecklenburg-Vorpommern, sec 61 and Staatsvertrag über die Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg, secs 36-37.

[53] See Germany, Federal Data Protection Act, sec 41 (1) and additionally Landesmediengesetz (LMG) Rheinland-Pfalz, sec 12; Landespressegesetz für das Land Mecklenburg-Vorpommern, sec 18a; Landespressegesetz Schleswig-Holstein, sec 10 and Pressegesetz des Landes Brandenburg, sec 16a.

[54] See Guideline 8.8 of the German Press Code at http://ethicnet.uta.fi/germany/german_press_code [Accessed 27 May 2016].

Chart Two: Subject Access and Journalism - Statutory Laws in EEA DPA Jurisdictions (n = 30)



Data Protection and Undercover Political Journalism

DPA Survey Question and Responses

The second question posed to DPAs set out a scenario involving the widely used, even if sometimes controversial, methodology of undercover investigation. Although hypothetical, it was deliberately based on a real-life case from the world of political journalism.[55] In sum, it stated:

> A journalist is investigating a far right political party following widespread claims that their true beliefs and tactics are much more extreme than their public face suggests. He intends to pose as supporter of the party and carry out undercover video recording of the party's activities.

DPAs were asked provide a general assessment of position of the journalist here as regards data protection. The five pre-formulated, standardized responses were as follows:

a. These journalistic methods would be illegal under data protection.

[55] Namely BBC Panorama's 2004 The Secret Agent documentary where Jason Gwynne spent six months undercover as a British National Party infiltrator. See BBC, 'Archive 2004: The Secret Agent' (2009) at http://news.bbc.co.uk/panorama/hi/front_page/newsid_8320000/8320387.stm [Accessed 27 May 2016].

b. These journalistic methods would be legal so long as (i) it was not possible to collect this information openly, (ii) the public interest in freedom of expression outweighed all interferences in privacy and (iii) the journalist obtained a permit from the Data Protection Authority for this activity.

c. These journalistic methods would be legal so long as (i) it was not possible to collect this information openly and (ii) the public interest in freedom of expression outweighed all interferences in privacy.

d. These journalistic methods would be legal so long the public interest in freedom of expression outweighed all interferences in privacy.

e. These journalistic methods would be legal so far as Data Protection is concerned.

Finally, as previously noted, in light of the potential complexity of the legal issues raised here, DPAs were alternatively able to state that the activity had a different relationship with data protection and then set out their own free-text answer.

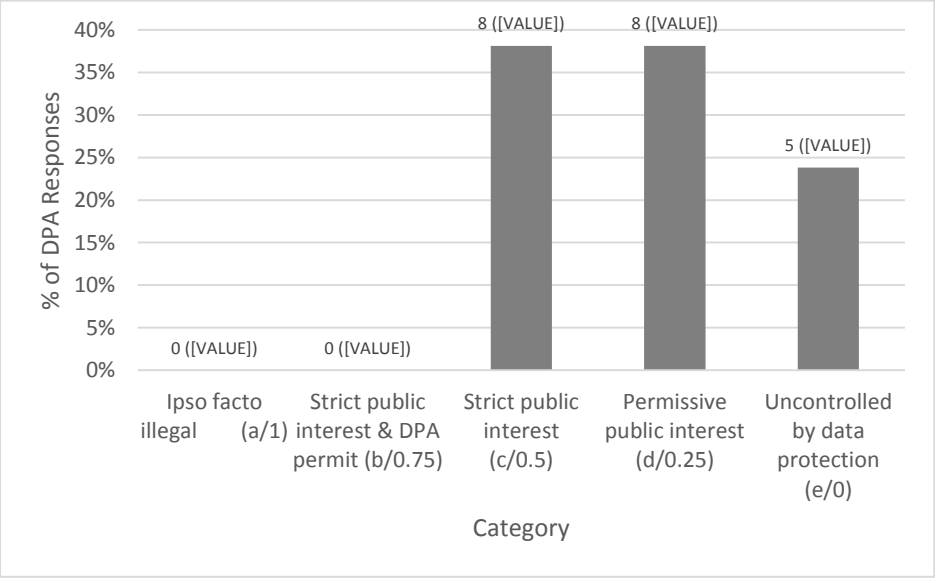
Twenty-one standardized responses were received here, which are summarized in Chart Three below and set out at individual DPA level in Table Two later in this article. As can be seen, no DPAs selected either of the first two categories. Eight DPAs (38% of the total) selected category c/0.5, eight (38%) selected category d/0.25 and finally six (24%) selected category e/0. In addition, some eight DPAs provided a free-text answer. Three of these answers appeared to suggest the need for a complex fact-specific inquiry here.[56] Meanwhile, one answer displayed a strong reluctance to engage with such an issue,[57] and two suggested that data protection law would not

[56] The German Brandenburg DPA signified this complexity simply by assenting to options (a) and option (e) in tandem. The Spanish Catalan DPA stated: "In some cases Spanish Constitutional Court considered this kind of undercover videorecording was illegal (v. qr. STC 12/2012). Nevertheless, in other cases considered that it was admissible (facts punishable)." The Polish DPA held: "The rules regarding journalistic investigation are not precisely prescribed by law. There is also not authority dealing with such questions. Therefore, any case has to be judged by court, taking into account the specific circumstances of the case".

[57] In sum, the Portuguese DPA stated that it "does not issue any permits for the data processing by the media companies concerning journalistic activity (only in other areas of the company, such as human resources, video surveillance systems, marketing, service subscriptions by clients). The limits and the legal conditions for this undercover case would be dealt by the media regulator not by the DPA".

apply here but that other related laws would regulate this area.[58] Finally, one answer assented to the proposition that the activity had a different relationship with data protection than any specified in the standardized responses[59], whilst another answer simply provided a full translation of that part of its national statute which regulates the interaction between data protection and the media.[60]

Chart Three: Data Protection and Undercover Political Journalism – EEA DPA Standardized Responses (n=21)



Position in Statutory Law

The undercover political journalism scenario above was purposively designed to raise issues as regards at least three default provisions within Directive 95/46. Firstly, the journalist here would

[58] The German Rhineland-Palatinate DPA held that "[h]is journalistic activities are without the control of the data protection authority; the data protection law is not applicable. But the journalist has to comply with the fundamental rights of personality, the right to determinate about one's own pictures and the civil law concerning damages (§§ 823, 826 German Civil Law). The persons who were observed can libel the journalist before the civil court if he violates the personality rights of party-members". Meanwhile, the Slovenian DPA stated that "[d]ata protection law generally does not apply in cases of covert recording. In Slovenia such is defined as a criminal act, and therefore the provisions of the Penal Code apply. Also, the general law on defamation and breach of privacy might apply".

[59] Namely, the French DPA. In the free-text section, this DPA did state that "[t]he processing would be illegal if the data has been collected by methods sanctions by criminal law. DP [data protection] law would not apply in the first place". However, this answer was officially confined to the situation of the covert social scientist outlined in note 79. It nevertheless seems likely that this DPA intended to indicate the same understanding also in relation to the covert journalist here.

[60] Namely, the Austrian DPA which provided an English translation of the stipulations set out in Austria, Federal Act Concerning the Protection of Personal Data (DSG), s. 48 (1).

clearly be collecting personal data (in the form of audio-visual recordings) from data subjects without notifying them of this. In principle, this would violate European data protection's proactive transparency rule which stipulates that when collecting information directly from data subjects, controllers must ensure that information as to their identity and the purposes of the intended processing is provided.[61] Secondly, much of the data would reveal information as to their "political opinions". As such information is deemed sensitive under Directive 95/46,[62] this processing would violate European data protection's default prohibition on the processing of such information[63] absent waiver by the data subject.[64] Finally, the non-transparent collection of information also sits in serious tension with the requirement to process data "fairly".[65] Although this is phrased in a completely open-textured form within the body of the Directive, Recital 38[66] states that "if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collection from him, must be given accurate and full information, bearing in mind the circumstances of the collection".[67]

Coding of jurisdictional statutory data protection law here is complicated not only by the inevitably rather general nature of the five potential categories detailed above but also by the fact that, in many instances, these laws set out different journalistic derogations as regards each of the

[61] Directive 95/46, art 10. The only exception relates to when the data subject already has this information which will clearly not be the case here.
[62] Directive 95/46, art 8. Given the nature of the example, it is highly likely that other types of data which European law considers sensitive will be captured such as information relating to criminal offences or that revealing philosophical beliefs.
[63] Directive 95/46, art 8.1.
[64] Ibid, art 8. Given that much of the information collected covertly will have been "manifestly made public" by the data subjects themselves (art 8 (1) (e)), such waiver could only be obtained through securing the explicit consent of the data subject for this processing (art 8 (1) (a)).
[65] Ibid, art 6 (1) (a).
[66] Recitals within EU legislation state the reason for a provision but are not directly substantively operative in and of themselves.
[67] Absent a strict public interest test being satisfied (category c/0.5), such processing is also likely to violate the default need for processing to be legitimated within the meaning of Article 7 of the Directive. In the exercise of essentially private as opposed to public law functions and in the absence of a consent or contract with the data subject, any such processing must be "necessary for the purposes of the legitimate interests pursued by the controller or by the third party to home the data are disclosed" unless "such interests are overriding by the interests for fundamental rights and freedoms of the data subject" (Directive 95/46, art 7 (f)). However, in practice, including this provision and derogations from it within the codings would make no different to the array presented below.

default data protection provisions. These laws were, therefore, coded into the most applicable category according to the following approximations. Firstly, given that the activity *ipso facto* conflicted with both the proactive transparency rule and the prohibition on processing sensitive data, the statutory law was generally coded according to the conditions set out for derogations from each of these provisions analysed, if necessary, cumulatively. Secondly, and as an exception to this, if the statutory law applied the fair processing requirement in full to the media then, in light of this provision's strong presumption in favour of transparent processing, the law was in any case coded at least within the permissive public interest derogation group (category d/0.25). Thirdly, if a special derogation from the fair processing principle was also present, then the coding according to the first rule was treated as paramount. In fact, as seen below, the patterns in the actual data rendered the second rule irrelevant in all cases and the third only potentially significant in one case.

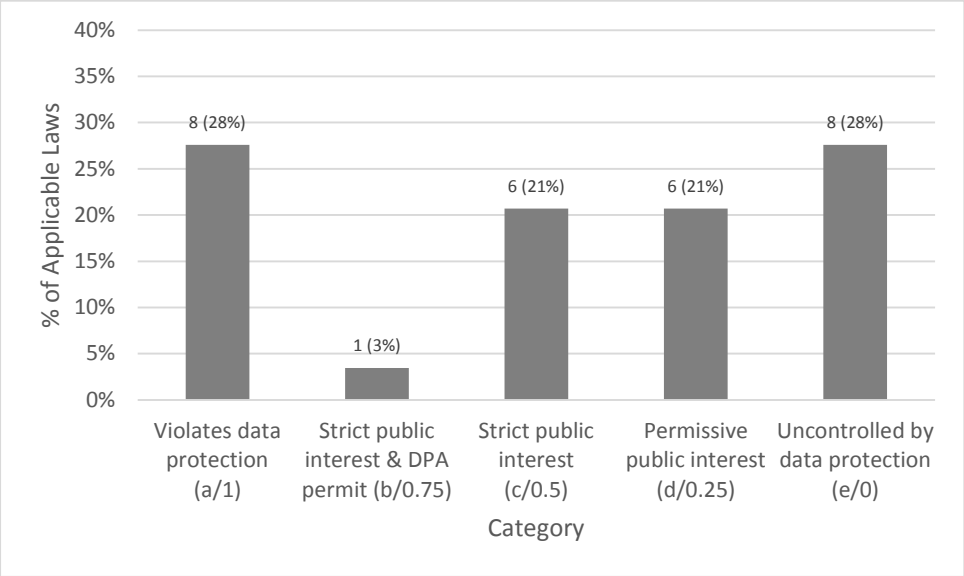
Drawing again on the more detailed analysis presented elsewhere,[68] the application of the rules above resulted in the following pattern. In eight DPA jurisdictions (28% of the total), statutory data protection law indicates that undercover political journalism of this type would always be illegal (category a/1). In four jurisdictions[69] this was due to the absence of any journalistic derogation as regards either the proactive transparency rule or the prohibition on processing data revealing political opinions. In contrast, in four others[70] only the latter provision applied in full to the media. It should be noted that in all these jurisdictions no journalistic derogation from the fairness provision was set out either. In one case (3%) statutory law stipulated that the journalistic exemption from the prohibition on processing data revealing political opinions not only needed to satisfy a strict test based on the public interest but also required a permit from the DPA (category b/0.75).[71] Again, the fairness provision also applied in full in this case. Six cases (21%) fell within category c/0.5 since a

[68] D. Erdos, "European Union Data Protection Law and Media Expression".
[69] Czech Republic, Slovakia, Slovenia and Spanish Catalonia.
[70] Hungary, Liechtenstein, Lithuania and Portugal.
[71] Greece.

strict public interest test had to be satisfied either, in three of these cases,[72] for exemption from the default prohibition on processing data revealing political opinions without consent or, in three more,[73] additionally also for an exemption from the proactive transparency rule. In all of these cases the general fairness provision was applicable to journalists, although in Italy it was subject to an interpretative gloss in favour of the media. In six further DPA jurisdictions (21%) derogation from both the proactive transparency rule and the political opinion processing rule depended on satisfaction of a more permissive test which was nevertheless still grounded in a public interest analysis.[74] These cases were therefore placed within category d/0.25. Finally, in eight cases (28%) there was an unconditional journalistic exemption from both the proactive transparency rule and the political opinion processing rule.[75] Additionally, in all of these cases a derogation from the fairness provision was also provided; indeed in all cases bar Austria[76] this was unconditional in nature. All these cases were, therefore, coded within category a/0. These results are summarized in Chart Four below and set out in full in Table Two below.

[72] Belgium, Cyprus and Luxembourg.
[73] Bulgaria, Estonia and Italy.
[74] France, Gibraltar, Ireland, Latvia, Malta and Poland. In two of these cases (France and Latvia) the fairness provision continued to apply in full to the media, whilst in the other four cases the same derogation applicable to the proactive transparency rule and the political opinion processing rule is also extended to the fairness provision.
[75] Austria, Finland, Sweden and the five German DPA jurisdictions. For full details of the German legislation see note 52 above.
[76] Ibid. In Austria the derogation here depended on satisfaction of a permissive test grounded in an analysis of the public interest.

Chart Four: Data Protection and Undercover Political Journalism – Statutory Law in EEA DPA Jurisdictions (n=29)



Comparing DPA Interpretation and Statutory Data Protection Provisions

Subject Access and Journalism

As regards the relationship between subject access and journalism, Table One below sets out for all the DPA jurisdictions which participated in the survey a cross-tabulation recording vertically the coding as per the formal statutory law and horizontally the coding as per the DPA's legal interpretation revealed in the 2013 survey. Any direct overlap between the two recorded values is signified by a darkly shaded box, whilst the two more lightly shaded boxes highlight the special case applicable to the German DPAs where two different interpretative answers could both be held to be in consistent with the provisions set out in statute. Using the figures disclosed on this table, it can be calculated that the average coded value along these dimensions is very similar, namely 0.44 in the case of the statutory law and 0.42 in the case of DPA interpretation. However, this commonality hides a good deal of other differences. Thus, despite the fact that the statutory laws in seven DPA jurisdictions (23% of the coded sample) mandated full application of subject

access to journalism (category a/1), all but one DPA (3%) avoided this. In contrast, an approximately equal number of statutory laws and DPA interpretations (4 (13%) compared with 5 (17%)) were placed within the polar opposite group of complete exclusion of the subject access right (category e/0). It is also apparent that DPAs were disproportionately attracted to the second most stringent possibility, namely, full access with the exception of information related to journalist sources. Thus, whilst only three applicable statutory laws (10%) mandated such an outcome, ten of the DPAs (34%) favoured it. A large and approximately equal number of DPA interpretations and statutory laws (11/38% compared to 9/30%) held that there was a need to balance subject access with freedom of expression (category c/0.5). Overall, only fifteen (or roughly 50%) of the cases fell within shaded boxes, with the highly specific regime of vicarious DPA access (category c/0.5) being the only category where a complete overlap between statutory law and DPA interpretation was evident. Turning to consider the spread of the data, whilst the standard deviation between the statutory laws was 0.37, it was 0.30as regards the DPA interpretations. This reflects a greater clustering of response from DPAs compared with what an analysis of local statutory law would predict. Finally, turning to correlative analysis,[77] the Spearman's rho between these two sets of data was 0.535 with a two-tailed significance value of 0.003. This indicates the presence of a clear and significant, yet far from overwhelming, relationship between journalistic provisions on subject access provisions as set out in local statute and DPA interpretation of the same.

[77] Non-parametric in light of the non-normal distribution of this and, indeed, all of the other variables in this research.

Table One: Subject Access and Journalism: Statutory Law vs DPA Interpretation

Statutory law (n = 30)→ DPA Interp. (n = 29)↓	Full access (a/1) **7 (23%)**	Access minus sources (b/0.75) **3 (10%)**	Vicarious DPA access (c/0.5) **2 (7%)**	Media rights may trump (d/0.25) **9 (30%)**	Media rights may or must trump (de/0.125) **5 (17%)**	Media rights must trump (e/0) **4 (13%)**
Full access (a/1) **1 (3%)**	·Cyprus	-	-	-	-	-
Access minus sources (b/0.75) **10 (34%)**	·Greece ·Slovakia ·Slovenia	·Italy ·Bulgaria	-	· Belgium · Estonia · Malta · Gibraltar	·Germany Schleswig-Holstein	-
Vicarious DPA access (c/0.5) **2 (7%)**	-	-	· Luxembourg · Portugal	-	-	-
Media rights may trump (d/0.25) **11 (38%)**	·Czech Republic ·Latvia ·Spanish Catalonia	·Hungary	-	·Ireland ·Liechtenstein ·Poland	·Germany Federal; ·Germany Brandenburg; ·Germany Mecklenburg-Vorpommern	·Lithuania
Media rights must trump (e/0) **5 (17%)**	-	-	-	·France	·Germany Rhineland-Palatinate	·Austria ·Finland ·Sweden
Free-text (1 response outside formal calculations)				·United Kingdom		

Data Protection and Undercover Political Journalism

Turning to consider the scenario exploring the interface between data protection and undercover political journalism, Table Two below sets out a similar cross-tabulation recording the codings calculated from local statutory law and from survey returns from the DPAs respectively. The disparities between these two dimensions are clearly much starker. Thus, whilst the average coded value of the statutory laws is 0.46, it is only 0.29 for the DPA interpretations. There is also far more clustering of values amongst the latter than the former, with a recorded standard deviation of 0.39 as regards statutory law but only 0.19 as regards DPA interpretations. DPAs entirely eschewed not only the possibility that covert political journalism was *ipso facto* illegal (category a/1) but also that such work required journalists to obtain a DPA permit for this alongside satisfying necessity and

general public interest criteria (category b/0.75). This is despite the fact that these, admittedly extreme, possibilities are set out in over 30% of relevant statutory laws. In contrast, as regards the polar extreme of unrestricted legality under data protection (category e/0), the gap between statutory law and DPA interpretation was much more minimal (eight statutory laws (28% of the coded sample) compared with five DPA interpretations (24%)). DPAs were disproportionately and equally attracted to the third and fourth categories respectively designating a strict (category c/0.5) and a more permissive (category d/0.25) exemption based on the public interest. Thus, in sixteen cases (76% of the coded sample) DPAs selected one or other of these categories, despite the fact that only twelve statutory laws (42%) were coded likewise. Nevertheless, turning finally to the correlative analysis, the Spearman's rho between these two sets of data was 0.583 with a two-tailed significance value of 0.006. This demonstrates that, within the narrow range of categories in which they clustered, the stringency of the statutory law was a good predictor of the stringency of a DPA's interpretative stance here.

Table Two: Data Protection and Undercover Political Journalism: Statutory Law vs. DPA Interpretation

Statutory law (n=29)→ DPA Interp. (n = 22)↓	Violates data protection (a/1) **8 (28%)**	Strict Public Interest & DPA Permit (b/0.75) **1 (3%)**	Strict Public Interest (c/0.5) **6 (21%)**	Permissive Public Interest (d/0.25) **6 (21%)**	Uncontrolled by Data Protection (e/0) **8 (28%)**
Violates data protection (a/1) **0 (0%)**					
Strict Public Interest & DPA Permit (b/0.75) **0 (0%)**					
Strict Public Interest (c/0.5) **8 (38%)**	·Hungary ·Liechtenstein ·Lithuania	·Greece	·Belgium ·Bulgaria ·Italy	·Malta	
Permissive Public Interest (d/0.25) **8 (38%)**	·Czech Republic ·Slovakia		·Estonia ·Luxembourg	·Latvia ·Ireland	·Germany Mecklenberg – Vorpommern ·Germany Schleswig-Holstein
Uncontrolled by data protection (e/0) **5 (24%)**			·Cyprus	·Gibraltar	·Finland ·Germany Federal ·Sweden
Free-text (7 responses outside formal calculations)	*·Portugal* *·Slovenia* *·Spanish Catalonia*			*·France* *·Poland*	*·Austria* *·Germany Brandenburg* *·Germany Rhineland-Palatinate*

Analysis

As elucidated above, the provisions applicable to journalism found in the statutory data protection laws within the EEA jurisdictions are highly divergent and, in many cases, clearly positioned at an extreme. It could be argued, however, that the survey evidence presented shows that, whilst taking into account local statutory provisions, EEA DPAs successfully resolve these difficulties through interpretation by ensuring that an equivalent and proportionate balance with freedom of expression is secured. However, although it is certainly clear that EEA DPAs are attempting to engage in a balancing exercise within this area, this perspective would fail to do justice to the incomplete, normatively contestable, opaque and precarious nature of the balance which is actually achieved.

The *incomplete* nature of this balance relates to the fact that, although almost all DPAs accept that data protection shouldn't be interpreted such that its core provisions are entirely applicable within in the journalistic area (category a/1), the same cannot be said for the other extreme of the complete non-application of data protection (category e/0). As can be seen both from Tables One and Two, EEA DPAs almost universally interpret the law so to avoid applying data protection in full to the media. The clear recognition of such a need sits in contrast to the interpretative stance of many DPAs as regards 'new media' activities (such as internet rating websites, online social networking, street mapping and certain types of search engine)[78] and also scholarly social science.[79] On the other hand, a number of DPAs indicated that, as regards both the subject access and covert political journalism questions, no data protection safeguards applied at all. The stance taken by these DPAs would appear to render a balancing of rights impossible. This suggests that, notwithstanding the existence of a right to data protection within the EU treaties themselves, DPAs have generally not (at least yet) been prepared to interpret the law such that this right is given horizontal effect vis-à-vis the media. However, although it is recognised that regulation of the media raises questions of particular national sensitivity, the resulting discrepant local

[78] Within the same survey as reported in this article, EEA DPAs were asked vis-à-vis hypothetical scenarios linked to these activities whether "[t]he general provisions of Data Protection law apply in full". In each case between almost half (47% as regards a rating website example) and almost all (93% in the case of a street mapping service) of the standard answers received indicated that the "general provisions of Data Protection law apply in full". These answers were in preference to three other options, namely: (i) that the law didn't apply at all, (ii) that Article 9 derogations and exemptions were engaged and (iii) that the general provisions had to be interpreted with regard for other fundamental rights including freedom of expression. For a full write-up of these results see D. Erdos "Data Protection Confronts Freedom of Expression on the 'New Media' Internet: The Stance of European Regulatory Authorities" (2015) 40 *E. L. R.* 531.

[79] Thus, within the same survey as reported here, DPAs were also asked to advise "[a] hypothetical social scientist researching widespread claims of racism within a police force [who] wishes to use covert methodology posing as a police recruit. Induction activities involving fellow recruits and police trainers would be secretly recorded, but the results of the study [would] be anonymized in so far as possible". Although the standardized responses were phrased slightly differently compared to that of the covert political journalism example above, it is nevertheless striking that a plurality of eleven DPAs (48% of the standardized total) agreed with the statement that "[s]uch research would be illegal as data would be collected directly from data subjects without their knowledge". This was despite the emphasis given by the hypothetical social scientist to ensuring anonymity, a safeguard which is much less likely to be followed in the case of the investigative journalist. A full write-up of this example will be published in work forthcoming by the author.

statutory framework which thereby results means that it is precisely in such an area[80] that data subjects are likely to find the potential direct effect of the data protection treaty right to be most valuable.

The high normative *contestability* of the DPA approach even where a balance has been attempted is highlighted by looking more closely at the response to the subject access example (Table One). As can be seen, although the most stringent possibility of full application of subject access was generally avoided, a large number of DPAs (34% of the standard sample) gravitated towards the second most stringent possibility set out, namely, full application of this right save from the disclosure of journalistic sources. Given that full application of the default subject access right will (at least if the source is a natural person as opposed to organization) pose a conflict with other data protection provisions such as fair processing, it is unsurprising that DPAs almost universally eschewed the possibility that the identities of sources would need to be revealed. At the same time, the granting of mandatory access to everything bar such source information would seem to give insufficient weight to the potential deleterious effects that might ensue if "every newsroom file would have to be open to inspection".[81] Writing as far back as 1985, Boulton wrote from a journalistic perspective candidly (and colourfully) on the possibility for such an eventuality to disrupt *bona fide* media practices:

> Consider: a particularly powerful John Citizen is under investigation by a computerised news team determined, in the public interest, to bring to light what Mr Citizen would prefer to keep in the dark … Mr Citizen knows his rights. He demands access to what the computers hold on him. The information supplied to the reporters has not yet been checked. Some of it is clearly libellous. Truth and untruth, copper-bottomed fact and malicious fantasy are intermixed, not

[80] Processing for the purposes of both crime prevention and national security are clearly other areas of high sensitivity. For recent CJEU case law highlighting increased EU involvement in these areas see the joined cases C-193/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Ors, Kärntner Landesregierung and Ors*, EU:C:2013:04 together with C-362/14 *Schrems v Data Protection Commissioner*, EU:C:2015:650.

[81] C. Thomson, G. Roscoe, K. Fulton and G. Mathias, "EC's 'catch-all' hold on press", *The Times*, 24 June 1991.

> yet sorted and separated in the complex editorial process it must all undergo before any of it is broadcast. Mr Citizen has the best lawyers money can buy. There's an injunction a gagging writ.[82]

Concerns relate not just to the potential for such an individual to inappropriately shut down lines of enquiry (whether through further recourse to the law or otherwise) but additionally the potential for a chilling effect whereby investigators might become wary about recording 'raw' data unsuitable for direct publication in the first place.[83]

Thirdly, responses to the subject access example are also indicative of the *opacity* and therefore unpredictability of the different balances adopted by the DPAs. In sum, even within the range of options that DPAs generally took to be interpretatively plausible, there was far from a direct relationship between the stringency of the formally adopted and transparently available statutory law and stringency of the relevant DPA's interpretative stance. To the contrary, four DPAs (14% of the coded sample) operating in jurisdictions whose statutes suggested such a need for an open-textured general balancing nevertheless indicated that subject access should apply to all but journalistic sources (category b/0.75).[84] In contrast, three DPAs (10%) operating in jurisdictions whose statutes set out no journalistic derogation from subject access (category a/1) nevertheless indicated that there was a need for an open-textured and general balancing between this and media freedom of expression (category d/0.25).[85]

Finally, the balances adopted are clearly *precarious* since they are often necessarily at considerable variance with the provisions found within local statutory law. Although DPAs are clearly unable to fully resolve this last problem themselves, this final issue has nevertheless been recognized by a number of them. Thus, the Czech DPA, which operates in a jurisdiction whose data

[82] D. Boulton, 'The Media: the dangers in data protection', *The Guardian*, 13 May 1985.
[83] For such an argument albeit made in relation to academic as opposed to journalistic investigations see E. Barendt, *Academic Freedom and the Law: A Comparative Study* (Oxford: Hart, 2010), p. 246.
[84] Belgium, Estonia, Malta and Gibraltar.
[85] Czech Republic, Latvia and Spanish Catalonia.

protection statute provides no express derogation for the media, has candidly stated that this "fact could justify the conclusion that the Personal Data Protection Act will thus apply, in the area of journalism, in the same way as to any other case of processing of personal data, thus requiring fulfilment (and penalising non-fulfilment) of all the duties set out in the Act".[86] Drawing on both constitutional norms and Article 9 of Directive 95/46 itself, this DPA goes on to clearly argue against such an approach. Nevertheless, such a 'work-around' is inherently incapable of ensuring the secure and legal certain[87] enjoyment of either freedom of expression and data protection which is particularly vital as regards the fundamental, yet often challenging, social activity that is journalism.

Conclusions and Future

European Union law requires that EEA Member States ensure a careful balance between data protection and journalistic freedom of expression. Whilst this outcome has often not been achieved within local data protection laws, the research presented sought to go further by exploring to what extent this has nevertheless been realised in the interpretation of the law adopted by statutory DPAs. The results demonstrated that DPAs do seek to balance journalistic freedom of expression alongside data protection even if this goes against provisions found within local statutory law. Nevertheless, the balancing attained remains incomplete and, as a result of its normatively contestable, opaque and precarious nature, in any case imperfect. Incompleteness arises from the fact that, as regards both the targeted question on subject access and the more general undercover political journalism scenario, a number of DPAs held that data protection safeguards were entirely absent. Normative contestability is particularly highlighted as regards subject access where approximately a third of DPAs held that only very limited journalistic derogations would be

[86] Czech Office for Personal Data Protection, *Position No. 5/2009 – Publication of personal data in the media* (2009) at https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1117&p1=1117 [Accessed 8 July 2016].
[87] According to the *EU Charter* it is a fundamental requirement that any limitation on either the right to data protection (art 7) or the right to freedom of expression (art 11) be "provided for by law" (art 52). Given that journalistic practices can implicate the essence of both these rights, this standard should be interpreted strictly here.

applicable here. Meanwhile, opacity derives that the fact that, although there was a relationship between the stringency of a DPA's response and the stringency of the local statutory provisions adopted, the former was nevertheless a long way from being predicable in light of the latter. Finally, the precarious nature of the balances reported relates to the fact that many of them are at very great variance with local statutory provisions.

It is clear that a large number of these challenges can only be effectively addressed through legislative as opposed to regulatory action. In light of this, it is essential that, during the process of implementing the General Data Protection Regulation, Member States act conscientiously to ensure that the new local laws which must be enacted under article 85 (2) – the cognate to article 9 of the existing Directive - do indeed effectively balance data protection with journalistic freedom of expression. Limitations as regards both of these rights must be carefully structured so as to adhere to the standards set out in both the *EU Charter* and national constitutional frameworks. In particular, they "must be provided for by law", respect the essence of the rights involved, comply with the principle of proportionality, be necessary and "genuinely meet … the need to protect the rights and freedoms of others".[88] Given that these provisions will now require notification to the Commission under article 85 (3), there is clearly also a role for that institution to police manifest violations of these common standards.[89] Alongside these legislative tasks there is also a need for greater regulatory attention to these matters. Therefore, in addition to action at local level, the new European Data Protection Board (a restyled and more powerful version of the current Article 29 Working Party) should produce a new Recommendation here, replacing its limited effort from 1997 and aimed at ensuring a more principled and consistent approach. Only such concerted regulatory and legislative action will ensure that the secure and certain enjoyment of rights is actually achieved in the critical, yet often fraught, area that is journalistic activity.

[88] *EU Charter*, art 52.
[89] In the case of the EU-affiliated EEA members, the EFTA Surveillance Authority could perform a similar role.