scripted

Volume 20, Issue 2, August 2023

Knowing me, knowing you: Opinions, reputation, DNA and other entangled personal data

Andrew Cormack

DOI: 10.2966/scrip.200223.7

Abstract

It's not uncommon for the same piece of personal data to relate to more than one individual. Opinions, feedback and reputation involve statements by one identifiable person about another; genetic data contain information about an individual, but also their relatives, ancestors and descendants; data about communications relate to both the sender and recipient; observations of one person may be used to make predictions about others. Privacy cases and papers have found these situations troubling, but analyse them by applying data protection law to a single data subject. This paper instead treats "entangled" personal data as involving multiple perspectives, examining how data protection principles apply simultaneously to different subjects of the same data. Where the perspectives are the same – as in a case on examination scripts – few problems are likely. Where there are significant differences this approach confirms the problems found by others but also suggests how these can be reduced: aligning the perspectives by changing data sources or processing, adopting voluntary limitations or safeguards. By quickly identifying problems that may not be apparent from a single-data-subject analysis, and

identifying possible mitigations, an entangled analysis provides theoretical and practical guidance: suggesting safer ways to use this increasingly common form of personal data.

Keywords
Data protection; opinions; reputation; genetic data; relational privacy

1 Introduction: Information About A Person?

Perhaps the most familiar phrase in data protection is that personal data "relat[e] to **an** identified or identifiable natural person".[1] As the added emphasis highlights, the data subject is singular. Yet many situations that academics and courts have found troubling involve data that relate to multiple data subjects: feedback to both giver and receiver, opinions to their holder and target, DNA to the donor and their relatives, communications data to senders and recipients. Big data techniques might even find unexpected correlative links between pairs of individuals.[2] Linked individuals may have similar relationships to the data and processing, for example social network "friends", or very different, for example a pupil's comment about a teacher. Knowing about one data subject tells us about the other(s).

This paper examines such "entangled" personal data simultaneously from both sides: considering the relationship between the paired purposes, lawful bases, principles, and data subject rights. If the two perspectives are significantly different then compliance – and wider ethical – difficulties are likely. Opportunities to alter data sources or processing to bring the perspectives closer indicate how problems might be reduced: where the perspectives overlap, voluntary self-limitation and extra safeguards can keep processing safely within this shared space. This approach reproduces the findings of both case law and

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter '*GDPR'*), Article 4(1).

2 Zexun Chen et. al, 'Contrasting social and non-social sources of predictability in human mobility' (2022) 13 Nature Communications <https://www.nature.com/articles/s41467-022-29592-y> accessed 10 June 2023.

academic research but might also suggest new ways to address the problems these identify.

The first section introduces situations involving entangled personal data that have been discussed in literature and case law and the very limited recognition of this factor. Entanglement is then added to each of the fundamentals of data protection law – principles, lawful basis, purpose and individual rights – revealing new analyses and insights. The literature examples are then revisited, finding that an entangled perspective both reproduces existing conclusions and suggests ways to address outstanding challenges.

2 Literature and Case Law

Todolí-Signes' "The Evaluation of Workers by Customers"[3] examines business models where customer evaluations provide the basis for both internal assessment and public reputation of individual workers. These include gig economy workers, public forums inviting customer comments on individual tradesmen, and feedback on both buyers and sellers in online marketplaces.[4,5] Such systems appear problematic for workers' rights: to privacy, non-discrimination, freedom from surveillance, to work and to access justice.[6] But legislation and case law indicate that "assessments on labour performance or on the professional behaviour, attitude and skills of natural persons gathered by an employer or posted online are protected under the GDPR".[7] Any processing must

---

3 Adrián Todolí-Signes, 'The evaluation of workers by customers as a method of control and monitoring in firms: Digital reputation and the European Union's General Data Protection Regulation' (2021) 160(1) International Labour Review 65.

4 Ibid 65.

5 eBay, 'Seller Ratings' <https://www.ebay.co.uk/help/buying/resolving-issues-sellers/seller-ratings?id=4023> accessed 10 June 2023.

6 Todolí-Signes (n 3) 68.

7 Ibid 70.

therefore have a lawful basis and – since a worker cannot give free consent to their employer[8] – possibilities are Article 6(1)(b) contract[9] and, perhaps, Article 6(1)(e) public interest for public professions such "doctors, architects and civil servants".[10] Both require all data collection and processing to be "necessary"[11] and to satisfy the Article 5 principles of adequacy, relevance and legitimacy. Todolí-Signes concludes

> only evaluations or information that are related to the professional capacity of the worker (making them relevant), are useful for checking such capacity (making them adequate), are not excessive (data are not repetitive or unnecessary) and are legitimate (not likely to affect a right or discourage its exercise) may be collected.[12]

But "[a]ny customer or employer assessment will be biased by the author's own emotions and particular preferences, which rarely allow for an objective analysis of the worker's performance": stereotyping and discrimination are obvious risks.[13,14] Thus GDPR requires "any information or assessment made by customers concerning facts or behaviors … outside the employment context must be immediately removed by the firm (or the data controller)":[15] a manual review

---

8 European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020), [21] <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 10 June 2023.

9 Todolí-Signes (n 3) 72.

10 Ibid 79.

11 Ibid 72.

12 Ibid 77.

13 Ibid 67.

14 Asri Özgümüs et. al, 'Gender Bias in the Evaluation of Teaching Materials' (2020) Front. Psychol. <https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01074/full> accessed 10 June 2023.

15 Todolí-Signes (n 3) 72.

cost[16] that employers and reputation forums must set against the savings from outsourcing traditional supervision by line managers.[17]

Todolí-Signes cites two contrasting cases applying data protection law to opinions: in *Mevaluate* the Italian Data Protection Regulator[18] rejected a proposed reputation register[19] whereas the German Constitutional Court[20] approved the balance of rights in the *Spikmich* feedback and discussion system for schools.[21] Key differences are the lawful basis invoked and the resulting choice of data sources and safeguards. The *Mevaluate* system was designed to help subscribers choose which organisations and individuals to contract with: as suppliers, partners, customers, or employees (paragraph 1.1). Many data sources – from national documentation to customer complaints (paragraph 1.3) – were to be gathered, published to subscribers, and summarised in an algorithmic "reputational rating" (paragraph 1.2). Its proposers considered consent (Article 6(1)(a)) as the appropriate lawful basis (paragraph 1.5) but the regulator ruled this could not be given freely where access to work might be affected (paragraph 2.3). Unlike national registration systems, *Mevaluate* was not backed by law that made processing a public task or legal obligation (paragraph 2.2). The "massive" range of data sources and their reliability and relevance were also questioned (paragraph 2.4). By contrast, *Spikmich* recognised that teachers could not consent when pupils expressed their opinions (paragraph 18) but claimed the school's

16 Ibid 77.

17 Ibid 66-67.

18 Garante per la Protezione dei Dati Personali, 'Piattaforma web per l'elaborazione di profili reputazionali – 24 novembre 2016' <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5796783> accessed 10 June 2023 (henceforth "*Mevaluate*").

19 Todolí-Signes (n 3) 76.

20 Bundesgerichtshof, Urteil des VI. Zivilsenats vom 23.06.2009 – VI ZR 196/08 (henceforth '*Spikmich*').

21 Todolí-Signes (n 3) 73.

legitimate interest (Article 6(1)(f)) in transparency and informed discussion (paragraph 24): paragraph 37 draws parallels with parent-teacher meetings. Such an interest must not be "overridden by the interests and fundamental freedoms of the data subject".[22] The court noted that only limited information and opinions were gathered: factual information about classes taught and average pupil ratings on fixed topics including "cool and funny", "popular", "motivated", "human", "good teaching" and "fair grades" (paragraph 1 – machine translation); that these were relevant to the teacher's professional, rather than personal, activities (paragraph 33); and that access was limited to pupils, teachers and parents with an interest in the discussion (paragraph 4). This struck an appropriate balance (paragraph 36). Importantly, feedback does not affect employment: the data quality is explicitly declared inadequate for "meaningful teacher evaluation" (paragraph 39).

Hallinan and Zuiderveen Borgesius[23] consider whether opinions are, and should be, subject to the GDPR's accuracy principle. Statements are provably correct or false but opinions are "probable facts". The authors' definition – "an assertion about an entity, built on facts about that entity subjected to some interpretative framework to produce new, probable facts about the entity"[24] – covers directly-expressed human opinions but also inferences and predictions by human or machine such as behavioural advertising profiles based on the activities and habits of other people.[25] In literature they find "no doubt that such opinions can qualify as 'personal data'"[26] but some argument that "opinions are,

---

22 GDPR, Article 6(1)(f).

23 Dara Hallinan and Frederik Zuiderveen Borgesius, 'Opinions can be incorrect (in our opinion)! On data protection law's accuracy principle' (2020) 10(1) International Data Privacy Law 1.

24 Ibid 6.

25 Ibid 7.

26 Ibid 5.

de facto, simply not the type of informational substance to which the accuracy principle can functionally relate".[27] Under their definition different factual starting points and different interpretive frameworks will affect the reliability of the resulting "probable facts": some will "provide more reliably precise and accurate personal data than others".[28] The authors consider this emphasises, rather than undermines, the importance of the accuracy principle: "to protect individuals against being irrationally or unfairly judged based on false representations".[29] Instead of discarding the principle we should recognise "the GDPR does not insist on absolute accuracy … rather, the GDPR requires a context-dependent analysis allowing certain leeway for controllers".[30] As in the case of *Nowak* "the assessment as to whether personal data is accurate and complete must be made in the light of the purpose for which that data was collected".[31]

Nowak also provides a rare explicit recognition that the same data can relate to more than one data subject. The European Court of Justice concluded that the examiner's written comments on an examination script were personal data of the candidate even though "those comments also constitute information relating to the examiner".[32] That dual nature was not relevant to the case – on whether the comments were accessible through a subject access request – but is the starting point for this paper's analysis.

Costello's "Genetic Data and the Right to Privacy: Towards a Relational Theory of Privacy?" considers a very different kind of data that relates to multiple

---

27 Ibid.
28 Ibid 8.
29 Ibid 9.
30 Ibid.
31 Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994 (henceforth "*Nowak*"), [53].
32 Ibid [44].

people: DNA. Analysing my genes also reveals personal information about my relatives, ancestors and descendants.[33] Privacy laws recognise genetic data as sensitive – it is one of the GDPR Article 9 special categories – and concepts of individuals "identifiable" from data should classify relatives as data subjects: exposed to their own risks, and entitled to their own rights.[34] But the "purely individualistic conception of privacy" underlying these laws ensures decisions are "taken by one individual, despite the consequences of that decision for a broader pool of people".[35] Ironically, the Article 9 special category provisions increase this individual focus.[36] Courts have recognised these broader impacts. In *S & Marper*, the European Court of Human Rights noted that "genetic data could be used to trace family members";[37] in *Gaughran*, unlike photographs and fingerprints, "the enduring and diffuse nature of DNA data … implicates the interests of a broader biological group".[38] Similarly in *Digital Rights Ireland* the European Court of Justice found electronic communications metadata "enabled the imputation of precise conclusions relating to the private lives of the individuals whose data have been retained—as well as those they communicated with";[39] in *Tele2/Watson* it offered "a portrait not only of the appellant but also a partial portrait of the individuals with whom they communicated".[40] In each case "privacy reductions for one individual may incur reductions in the privacy of others".[41] To capture these "contagious" consequences, recognised by the courts,

---

33 Róisín Costello, 'Genetic Data and the Right to Privacy: Towards a Relational Theory of Privacy?' (2022) 22(1) Human Rights Law Review 1, 2.
34 Ibid 13.
35 Ibid 2.
36 Ibid 12.
37 Ibid 15.
38 Ibid 16.
39 Ibid 17.
40 Ibid 18.
41 Ibid 19.

Costello proposes an assessment of "relational privacy" that includes harm to others.[42,43] But practical problems remain in both control and enforcement: how distant a relative can assert their rights to control 'my' genetic data,[44] will any individual have sufficient interest in enforcing those rights,[45] and what is an appropriate sanction when a privacy breach is caused by a data subject's insecure or inappropriate handling of the multi-party data?[46] Nonetheless Costello concludes "a concept of relational privacy may be the approach best equipped to deal with the privacy impacts of genetic data, and indeed the networked impacts of privacy infringements in the twenty-first century more generally".[47]

3 The "Entangled" Perspective

None of these articles and cases doubts that their topic is personal data subject to the General Data Protection Regulation (GDPR). Opinions and feedback are not – and, according to Hallinan and Zuiderveen Borgesius, should not be[48] – excluded by their informality or subjectivity: the Article 29 Working Party's 2007 Concept of Personal Data "includes 'subjective' information, opinions or assessments"[49] and the 2017 ECJ judgment in *Nowak* confirmed that personal data "potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to

42 Ibid.
43 Ibid 22.
44 Ibid.
45 Ibid 21.
46 Ibid 23.
47 Ibid 22.
48 Hallinan and Zuiderveen Borgesius (n 23) 9.
49 Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (20 June 2007), 6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 10 June 2023.

the data subject".[50] Online identifiers and genetic data are explicitly mentioned in GDPR Article 4(1)'s examples of personal data.

But most authors focus on a single data subject: the target of an opinion or feedback, the donor of a DNA sample and the person of interest in data retention cases. Thus *Spikmich* concentrates on the teacher, *Mevaluate* on the worker, and *Nowak* finds the examiner's written comments, as well as the candidate's answers, "constitute information **relating to that candidate**" [emphasis added].[51] Other parties' rights are occasionally implied: Hallinan and Zuiderveen Borgesius refer to political opinions being the speaker's special category data under Article 9 GDPR or protected speech under Human Rights laws.[52] Only *Nowak* explicitly identifies two data subjects: "finding that the comments of the examiner … constitute information which … is linked to that candidate is not called into question by the fact that those comments also constitute information relating to the examiner".[53] Closer examination of these situations, where "[t]he same information may relate to a number of individuals and may constitute for each of them … personal data",[54] reveals common features that help address both theoretical and practical concerns. Here we refer to such information as "entangled personal data".

Intervening processing need not destroy entanglement. For example: seller ratings might depend on the percentage of positive customer feedback; teacher assessments use the improvement in their pupils' scores; individual preferences be inferred from observed behaviour of social network

---

50 Nowak (n 31), [34].
51 Nowak (n 31), [42].
52 Hallinan and Zuiderveen Borgesius (n 23) 10.
53 Nowak (n 31) [44].
54 Ibid [45].

"friends".[55,56,57] Such processing might seem to separate sets of personal data – one about pupils, one about teachers – but actually makes their entangled nature more significant. Combining data from multiple sources may reduce the impact on those individuals but correspondingly increases the statistical weight and intrusiveness for the individual target of the aggregated data. *Nowak* confirms that purpose, not mathematical or procedural complexity, matters: "a representative survey, to obtain information that is independent of that person" is fundamentally different from an examination "to determine and establish the individual performance of a specific person".[58] Likewise, though both individuals will often be "identified or identifiable" to the same data controller – the school in *Spikmich* can identify both the pupil/parent and teacher; the reputation platform in *Mevaluate* both the customer and service provider – the entangled approach also yields insights in situations, such as DNA, where this is not true. Wherever there may be identifiable individuals at both ends of the chain their entangled interests in the data should be considered.

4 Entanglement and the GDPR

This paper therefore proposes "entanglement" as a lens – perhaps more accurately a pair of spectacles! – to examine processing proposals and activities. Where personal data relate to multiple data subjects, instead of analysing the GDPR requirements for individuals (or classes) separately we consider both simultaneously. This reveals both challenges and opportunities likely to be

---

55 eBay (n 5).

56 Laura Goe and Andrew Croft, 'Methods of Evaluating Teacher Effectiveness' (*National Comprehensive Centre for Teacher Quality*, March 2009) <https://gtlcenter.org/sites/default/files/docs/RestoPractice_EvaluatingTeacherEffectiveness.pdf> accessed 10 June 2023.

57 Hallinan and Zuiderveen Borgesius (n 23) 7.

58 Nowak (n 31) [41].

missed by single-sided analysis. Distance or differences between the two perspectives highlight potential problems: matches or overlaps indicate where safeguards and obligations have double benefit. Adjusting processing, data sources or safeguards to bring the perspectives closer should reduce difficulties: adding new controls, safeguards or voluntary limits can increase the amount of overlap and keep processing safely within it.

This section considers familiar basic requirements of the GDPR – principles (Article 5), lawful bases (Article 6), purpose (Article 6(4)) and individual rights (Chapter III) – but applies them to entangled personal data. Examples are from the literature review above. The final sections show how an entangled perspective can extend the conclusions, guidance and safeguards derived from a single data subject analysis.

4.1 Entangled Principles

The GDPR's substantive content begins with six principles in Article 5(1): lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality. Sometimes considered a seventh principle is accountability (Article 5(2)): the data controller must be "responsible for, and … able to demonstrate compliance with" the other six. This is a proactive duty to design and operate systems that comply with the principles, not just a warning of retrospective sanctions if they are breached. Considering accountability for entangled data – addressing simultaneous obligations to multiple individuals – provides new insights. The principles of fairness, accuracy and security are discussed here; lawful basis, purpose and individual rights have dedicated sections below.

The UK Information Commissioner describes the Article 5(1)(a) fairness principle as meaning "you must not process data in a way that is unduly

detrimental, unexpected or misleading".[59] Fairness is supported by the Article 5(1)(b) requirement that data be "collected for specified, explicit and legitimate purposes". Thus – emphasised by the Article 5(1)(a) requirement for transparency – a person whose opinion (whether express or inferred) is collected must be informed of *all* purposes for which it will be used, even those that primarily affect other, entangled, data subjects. Todolí-Signes notes that expressed opinions are affected by external factors: knowing their response will affect the target might tempt an opinion holder to 'send a message' or even "retaliate[e]".[60] In a platform like *Spikmich*, pupils might respond differently if invited to rate 'course materials' rather than 'course teacher'. More customers might complete a feedback form that directly rewards (or punishes) the individual worker than one providing sentiment information to the employer. It is questionable whether processing feedback that was deliberately constructed to produce a particular result is either relevant (as required by Article 5(1)(c)) or accurate (Article 5(1)(d)) for the worker. But the entangled perspective asks whether processing that changes a person's behaviour (here the feedback provider) is even fair to them. Reversing *Spikmich*: a teacher might be reluctant to tell a pupil they need to work harder if they know the pupil's feedback will affect their own assessment. Such a behaviour change might well be "unduly detrimental" to both if educational results suffer because necessary, critical, feedback is withheld.

An entangled perspective on fairness highlights that even processing that has no direct effect on a data subject can still be unfair if its existence causes an

---

[59] Information Commissioner's Office, 'Principle (a): Lawfulness, fairness and transparency' (1 January 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/> accessed 10 June 2023.

[60] Todolí-Signes (n 3) 67.

"unduly detrimental" behaviour change. This might equally apply to unentangled situations if the existence of a secondary processing purpose makes the single data subject change behaviour towards a primary purpose. Medical or other sensitive websites should perhaps be particularly careful about using browsing data for secondary commercial or even site-improvement purposes.

The Article 5(1)(d) accuracy principle appears straightforward: "Personal data shall be … accurate" contrasted with "personal data that are inaccurate". According to the Article 29 Working Party "[i]n general, 'accurate' means accurate as to a matter of fact".[61] The Article 19 rectification process reflects this binary view: the data controller must "communicate any rectification … to each recipient to whom the personal data have been disclosed" presumably so that recipients can replace "inaccurate" data in their systems by the "accurate" value. But Hallinan and Zuiderveen Borgesius define "opinions" as precisely those personal data that do not "mirror an objective, external reality".[62] Here they find "the GDPR requires a context-dependent analysis":[63] emphasising Article 5(1)(d)'s "accurate … having regard to the purposes for which they are processed".[64] In entangled situations, however, the contexts of "collected"[65] and "judged"[66] may have different accuracy requirements for the same data or, indeed, contradictory understandings of accuracy. A true record of a false opinion is accurate from the opinion-holder's perspective but inaccurate from

---

61 Article 29 Working Party, 'Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc v Agencia Española de Protection de Datos (AEPD) and Mario Costeja Gonzalez' C-131/12' (26 November 2014), 15 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf> accessed 10 June 2023.

62 Hallinan and Zuiderveen Borgesius (n 23) 4.

63 Ibid 9.

64 GDPR, Article 5(1)(d).

65 Nowak (n 31) [53].

66 Hallinan and Zuiderveen Borgesius (n 23) 9.

that of its target. Comparing accuracy requirements helps data controllers identify these mismatches: it may also suggest possible remedies. Adjusting processing might better align the two sides' requirements (e.g. reducing the weight given to conflicted sources); accuracy could be applied in favour of the side with the stricter requirement (e.g. *Spikmich's* unconditional option for teachers to block individual ratings[67]); the data source could be improved or rejected; or, if harm is limited to specific data items, the Entangled Rights processes discussed below used to mitigate those. At the very least, an entangled perspective on accuracy reveals situations where data controllers must take particular care.

The Article 5(1)(f) principle requiring that personal data be "processed in a manner that ensures appropriate security … using appropriate technical or organisational measures" is normally applied to storage and access mechanisms. Applying an entangled analysis – considering the overlapping needs of multiple data subjects – recalls Costello's concern that the actions of one data subject might harm others.[68] The security principle applies to the data controller, not data subjects, so any controller whose activities create these "contagious" risks[69] might be required to take "appropriate measures" to mitigate them. For example, a service using DNA samples to map family trees could apply different disclosure or notification processes for relatives likely to be alive, providing some "protection against unauthorised or unlawful processing".[70] Proactive measures by data controllers reduce the need – rightly considered "impractical" by Costello[71] – to determine which individuals in the entangled group are at risk of

---

67 *Spikmich* (n 20) [39].
68 Costello (n 33) 23.
69 Ibid 22.
70 GDPR, Article 5(1)(f).
71 Costello (n 33) 22.

significant harm. Unlike tort-based systems, GDPR enforcement does not require individuals to claim damage: regulators can investigate industry sectors and, if necessary, sanction data controllers for non-compliance.[72] This approach could protect individuals without relying on "individually enforceable and divisible rights".[73]

4.2 Entangled Lawful Bases

GDPR Article 5(1)(a) requires that all processing be "lawful": covered by one of the six lawful bases in Article 6(1)(a). Each has its own requirements and safeguards: the *Spickmich*[74] and *Mevaluate*[75] cases illustrate how these can improve processing. Article 6(1)(f) "necessary for a legitimate interest" shows that constraining *Spickmich* feedback options reduced risk without affecting the platform's function; it also provided the framework for the rights-balancing assessment that the Court concluded was favourable to the platform. Article 6(1)(a) "consent" must be freely given[76] which raised immediate doubts about the validity and safety of processing in *Mevaluate*. Entangled processing is likely to involve two lawful bases: one for each (group of) data subjects. Examining these simultaneously, considering how their expectations and requirements interact, can provide further information, safeguards and, in some cases, reassurance.

The simplest situation is the case of *Nowak*, which entangles the data protection rights of a candidate in – as the judgment repeatedly stresses – a "professional examination" and the examiner commenting on their answers. The judgment does not state an explicit lawful basis for either processing but the

---

72 GDPR, Article 57.
73 Costello (n 33) 10.
74 *Spikmich* (n 20).
75 *Mevaluate* (n 18).
76 GDPR, Article 7(4).

purpose "to evaluate the candidate's professional abilities and his suitability to practice the profession concerned" seems strongly linked to a "public interest" (now GDPR Article 6(1)(e)) in the skills of accountancy practitioners, which would apply to both taking and marking this exam.[77] In particular, both parties should have had similar expectations about and commitment to the process, the safeguards on both arise from the same source, and the two contexts have similar requirements for data quality and reliability.

This contrasts with *Mevaluate*, where a plausible analysis (not adopted by the platform) would be that some information sources – for example customer complaints – were provided by Article 6(1)(a) consent but the planned use of the resulting information was Article 6(1)(b) necessary for contract. Between this pair of lawful bases there are significant differences in the parties' freedom to participate (or not), the expectations of data quality, and the safeguards applied to processing. Where personal data are collected by consent the data subject can choose to be silent, selective, or untruthful. This is, in effect, their safeguard against harm from further processing. An individual whose reputation rating is necessary for contract may, however, be seriously harmed by such data and has no way – since the Article 21 right to object does not apply – to prevent its processing. The data source has practical and proactive safeguards in their own hands: those for the worker (such as the Article 16 right to rectification) are retrospective, apply after damage has been done, and require action by a regulator or court. The judgment mentions registers backed by law: their collection necessary for a legal obligation (Article 6(1)(c)) might be more compatible with necessary for contract but data provided by consent (Article 6(1)(a)) are still problematic. In *Mevaluate* the Data Protection Authority did

[77] Nowak (n 31) [38].

identify the data quality problem by close examination of the proposed sources[78] but considering the entangled lawful bases provides quicker identification and possible ways to remedy it.

An entangled analysis of *Spickmich* shows the benefits. Article 6(1)(f) legitimate interest was chosen for processing teachers' personal data:[79] pupils' comments appear to be optional so covered by Article 6(1)(a) consent. Considering these two bases as entangled shows that, while they are not identical, voluntary limits on processing and additional safeguards by the platform and data controllers may reduce the mismatches to an acceptable level. Avoiding – formally, and especially in practice – any processing necessary for (the teacher's employment) contract is critical. As in *Mevaluate*, data quality is a concern but *Spickmich* addresses this by constraining both the topics and form (scores, not free text) of the students' views. The teacher's ability to freely mark inputs as unreliable and not to be processed further brings the teacher's and pupil's direct controls into closer alignment.[80] This unconditional opt-out is a stronger safeguard than the Article 21 right to object, which does apply to legitimate interest processing; being more granular, the opt-out also benefits the platform by permitting processing of opinions that are not contested. Finally, Article 6(1)(f)'s three-stage test – that the purpose be legitimate, that processing be necessary for that purpose, and that the processing not be overridden by the data subject's interests and rights – helps all parties confirm that the differences between the two lawful bases have been sufficiently mitigated.

Aligning lawful bases is helpful at the start of processing but some combinations of lawful bases may also create problems at its end, when one of

---

78 *Mevaluate* (n 18) [2.5].
79 *Spikmich* (n 20) [42].
80 Ibid [39].

the entangled bases is lost. This is most likely to occur following the exercise of a right of objection or erasure, so is discussed under Entangled Remedial Rights below.

4.3 Entangled Purposes

As well as a lawful basis, under Article 5(1)(b) all processing must have at least one "specified, explicit and legitimate purpose"; any "further processing" must not be "incompatible" with those specified during collection. Further processing typically involves the same data subject but Article 6(4)'s factors for (in)compatibility seem particularly relevant for other, entangled, data subjects. Unless these can give valid consent, the controller must consider:

> a. Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
> b. The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
> c. The nature of the personal data, in particular whether special categories of personal data…;
> d. The possible consequences [whether direct or indirect] of the intended further processing for data subjects;
> e. The existence of appropriate safeguards…[81]

As the Article 29 Working Party noted, new purposes are not prohibited,[82] but their focus on "what a reasonable person would find acceptable"[83] is a reminder

---

[81] GDPR, Article 6(4).

[82] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (00569/13/EN WP203), <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> p. 21 accessed 10 June 2023.

[83] Ibid 23.

that the entangled "reasonable person" may not even be involved in the initial collection and processing. An entangled purposes approach favours situations where the different groups are processed for related purposes; where they have similar relationships with the data controller; where the understanding, meaning and significance of the (non-special-category) personal data are similar; where the consequences – resulting from processing and from its entangled nature – are understood, necessary and proportionate; and where safeguards can be applied. Situations with significant differences between two perspectives on any of these factors are likely to be problematic.

This confirms Todolí-Signes' concern about using express customer evaluations in worker performance assessments. Although the purposes may appear linked – referring to the same work – the data subjects' relationships to the controller/employer are very different. Feedback is normally the last act in the customer's receipt of a service: the employee continues to depend on the employer for future work and income. The customer is likely to perceive their comment as informal, inconsequential, and ephemeral, unconcerned about objectivity[84] even though the same information may become a permanent part of the employee's formal record. For the employee there are significant consequences which – because they are the intended result of the processing – are hard to mitigate by safeguards.

This might be contrasted with a possible alternative system within the workplace that assesses a manager based on the measured productivity of their team. Here the relationships and consequences for the two sides are similar, it should be possible to establish a shared understanding of the meaning of the data and to provide safeguards – such as review and pseudonymity – for factors and

[84] Todolí-Signes (n 3) 67.

situations such as system outages, sickness or disputes that make the measurement an unreliable reflection of the performance of either workers or manager.

4.4 Entangled Rights

Articles 13 to 22 of the GDPR establish so-called "rights" of data subjects. In fact, Articles 13 and 14 create proactive duties on data controllers to provide information to all data subjects including passive ones; while Articles 15 to 21 create rights – of subject access, rectification, erasure, restriction, portability and objection – that individual data subjects may actively exercise. Article 22(1) on automated decision-making, though expressed as a "right", is now interpreted as a "general prohibition".[85] Article 12 requires data controllers to "take appropriate measures" to satisfy their duties and to enable data subjects to exercise their rights. However, as we discuss first, in entangled situations the informational duties in Articles 13 to 15 may themselves conflict with data protection expectations. Novel combinations of the remedial rights in Articles 16 to 21 may be needed to maintain safeguards.

4.4.1 Entangled Information Duties

Entangled data will often be gathered when one data subject is present but others are absent.[86,87] This creates proactive information duties under both Article 13 "collected [including by observation] from the data subject" and Article 14 "not

[85] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (6 February 2018), 23 <https://ec.europa.eu/newsroom/article29/redirection/document/49826> accessed 10 June 2023.

[86] Hallinan and Zuiderveen Borgesius (n 23) 3.

[87] Costello (n 33) 5.

been obtained from the data subject" for example targets of feedback and DNA relatives. These duties include providing specific information about the processing, commonly referred to as "metadata". In addition, Article 15 entitles individuals to make subject access requests and receive both metadata – largely repeating the Article 13 and 14 information – and the actual personal data being processed.

All three articles require (Articles 13(1)(e), 14(1)(e) and 15(1)(c)) the controller to tell the provider of personal data "the recipients or categories of recipients …, if any"; according to the EDPB "[t]he controller should … generally name the actual recipients".[88] But for feedback and opinions those "actual recipients" include the individual feedback targets: likely to be identifiable either directly from the disclosed information or "combined with other information available" to the data source.[89] Even "categories of recipients" may constitute personal data for small categories (e.g. "form teachers") where identification, using the opinion holder's knowledge, is "pretty conclusive".[90] These mandatory metadata disclosures themselves involve entangled processing of data relating to multiple individuals with different expectations.

An individual providing entangled data will often already know the identities of others it relates to, so disclosing recipients to them adds little risk. Disclosure might even be exempt as "the data subject already has the information" (Articles 13(4) and 14(5)(a)). However, Articles 14(2)(f) and 15(g) require the reverse disclosure "from which source the personal data originate", which could be a significant privacy breach when the source is an individual. As

---

88 European Data Protection Board, 'Guidelines 01/2022 on data subject rights – Right of Access' (18 January 2022), [115] <https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf> accessed 10 June 2023.

89 Article 29 Working Party (n 49) 13.

90 Ibid.

well as direct risks of harm, knowing that they may lose anonymity could cause the source to change their behaviour, as discussed above. Unlike recipient information, there is no mention of source categories so, again, an individual source will often be identified or identifiable from the disclosed metadata, especially as the EDPB suggests that any generic Article 14 information should be made case-specific when responding to an Article 15 subject access request.[91] *RW*[92] appears to confirm that the requester can always opt to receive "information about the specific recipients" (46), unless this is "impossible" (48): it is not clear whether identifying individuals would constitute legal impossibility.

Article 15 does recognise the risks of disclosing entangled data in Article 15(4)'s instruction that "the right to obtain a copy … shall not adversely affect the rights and freedoms of others". Where necessary, according to the EDPB, "information concerning others [may be] rendered illegible" before disclosure.[93] But this only applies to the Article 15(3) "copy", not to the source and recipient metadata that must be disclosed under Article 15(1) and, at collection time, Articles 13(1)&(2) and 14(1)&(2).[94] Some contexts might involve an Article 14(5)(d) "statutory obligation of secrecy" but the problem is highlighted by Article 14(5)(c): disclosure *is* "expressly laid down by Union or Member State law" but that law (the GDPR itself) does *not*, in entangled cases, "provide[] appropriate measures to protect the data subject's legitimate interests".

Considering entangled information rights reveals risks in disclosing individual recipient and, particularly, source identities, but the mandatory nature of the disclosures makes the risks hard to mitigate. Data controllers might

---

91 EDPB (n 88) [118].
92 Case C-154/21 *RW v Österreiche Post AG* [2023] ECLI:EU:C:2023:3.
93 EDPB (n 88) [170].
94 Ibid 4.

design processing and systems so routine disclosure of source identity is not "necessary to ensure fair and transparent processing", providing a partial exemption under Article 14(2). But there are no clear grounds to refuse or redact an Article 15(1)(c) or (g) subject access request for metadata that is another person's personal data. Where metadata disclosure under Articles 13 to 15 could create serious risk to individuals, entanglement may indicate that data controllers should simply avoid such processing.

4.4.2 Entangled Remedial Rights

Responsibility for preventing harmful or unfair processing rests primarily with the data controller:[95] individuals should not be required "to continually act as unpaid proofreaders of their records".[96] The role of the Article 13 to 15 information rights – to know who is processing information, why, how, and the actual values – is to help individuals identify when their particular circumstances may make otherwise safe processing inaccurate, harmful or unlawful.[97] Affected data subjects can then exercise their remedial rights – respectively of rectification (Article 16), objection (Article 21) and erasure (Article 17) – to prevent further harm. An entangled perspective on these rights suggests how they can be used – sometimes in novel ways – to provide mutual safeguards for multiple data subjects even where entangled interests require limiting the information disclosed under Articles 13 to 15. It also identifies situations where one data subject's exercise of a remedial right may conflict with the rights of others.

Unlawful processing will usually be apparent from metadata – e.g. purpose, types of source and recipient – that can be disclosed even in entangled

---

95 Todolí-Signes (n 3) 77.

96 Daniel Solove, 'The Limitations of Privacy Rights' (2022) GW Paper Series 2022-30, 25 https://scholarship.law.gwu.edu/faculty_publications/1605/ accessed 10 June 2023.

97 EDPB (n 88) [10], [12].

situations. However, as discussed above, entanglement may raise new issues for fairness and accuracy of processing. For example: do different purposes of collection and use make processing unfair; can we define, let alone correct, instances of "inaccuracy"? Normally, the data controller would resolve these issues by comparing the parties' perspectives on the data and seeking a common understanding. But where both parties are individual data subjects such discussions may be unlawful (if content needs to be redacted) or impossible (if a party refuses to engage). Can the significance and accuracy of an opinion be understood without revealing individual identities? Is it fair to process data that must be redacted before being shown to the person it impacts? What should happen when one person's remedial rights of objection or erasure will infringe another's rights or interests?

Hallinan and Zuiderveen Borgesius consider the purpose of the accuracy principle is to "ensure fair processing" and, in particular, "ensure individuals are not falsely represented via their data doubles".[98] In an entangled situation, accuracy may legitimately be disputed or even undefinable; choosing a single 'correct' value will "falsely represent" and could harm the holder of the opposing view. Fortunately, the GDPR's remedial rights can avoid harm while leaving accuracy unresolved. Article 18's right to restriction can be applied where "the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data". During restriction, normal processing of the contested data is prohibited. Where entanglement means accuracy cannot be defined, or the data controller cannot "verify" it, this text seems to allow an indefinite "period" of restriction. Prohibiting processing should prevent harm; processing that is still permitted

[98] Hallinan and Zuiderveen Borgesius (n 23) 9.

under Article 18(2) – by consent, to support legal claims, individual rights or important public interests – could be made safer by attaching the objecting party's rebuttal (Todolí-Signes notes "the worker's right to explain the situation and place the assessment within context"[99]) or the controller's conclusion (for example that this is an accurate record of a mistake, in the UK Regulator's example[100]).

A right of restriction is also associated with the rights to object (Article 18(1)(d)) and erasure (Article 18(1)(b)&(c)) but these raise a deeper issue when processing entangled data. As discussed above, an Article 6 lawful basis is required in respect of each data subject. A successful objection – to processing based on a public or legitimate interest – or erasure – on termination of contract or withdrawal of consent – removes one of these bases. Even if the other data subject's lawful basis remains intact, continued processing of the entangled data may be unlawful. Anonymising the data might be an option: removing entanglement because the data are longer personal to the objecting/erasing party. But anonymisation or, especially, erasure might well harm the second data subject if they want the data preserved, unmodified, for a purpose listed in Article 18(2): "the establishment, exercise or defence of legal claims or … the protection or rights of another natural person". This Article – which permits processing even of restricted data – foresees entangled situations where "another … person" could be affected by anonymisation, erasure or, indeed, rectification. But it contains no mechanism to inform those persons when an objection or erasure may affect evidence supporting their claim or rights. Hallinan and Zuiderveen Borgesius see "fertile ground" for further research on rights to

---

99 Todolí-Signes (n 3) 77.

100 Hallinan and Zuiderveen Borgesius (n 23) 3.

rectification:[101] whether entangled data subjects have a right to be informed of pending changes might be one topic. Data controllers should at least assess how their entangled processing might be affected by the exercise of individual rights, and plan how they will respond.

5 Discussion: Applying Entanglement

An entangled perspective on opinions, employee monitoring and genetic data – studied respectively by Hallinan and Zuiderveen Borgesius, Todolí-Signes and Costello – confirms those authors' concerns and conclusions, but also suggests how their analyses and safeguards can be extended.

Hallinan and Zuiderveen Borgesius' broad definition of "opinions" includes many kinds of entangled data, from one person's express statement about another to an algorithm's inference about one individual from the observed behaviour of others. None of these "reflect a known empirical reality"[102] so their accuracy cannot be assessed as simply true or false. Instead, the authors conclude "the purpose of collection and processing will determine the perspective from which the relevant level of precision should be decided".[103] But considering the opinion as entangled personal data questions whether there is a single "purpose of collection and processing" or whether collection (from opinion holder) and processing (to opinion target) might demand different "level[s] of precision". The authors note that an "ethical reflection" may be needed to resolve conflicts between accuracy and other "relevant rights and interests of the parties involved" such as free political expression.[104] However

[101] Ibid 9.
[102] Ibid 5.
[103] Ibid 4.
[104] Ibid 10.

entangled accuracy provides a way to identify and resolve these conflicts within data protection law: perhaps simpler than balancing among different fundamental rights. Any significant difference in the "margin[s] of error in precision"[105] required by the contexts of opinion holder and opinion target identifies a risk, especially if the target's accuracy requirement is higher than that of the holder. Proactive mitigations – such as changing or constraining the source of data – may be found by considering, and possibly altering, the entangled principles or lawful bases; entangled individual rights may provide retrospective remedies for individual opinions.

Todolí-Signes analyses the use of customer comments to assess the performance of individual workers. Treating comments as the worker's personal data whose processing is "necessary for the performance of the (employment) contract"[106] the GDPR principles prohibit the use of any comments that do not relate to the performance of the work; are discriminatory or otherwise illegitimate; are inaccurate, incorrect or untrue; or are otherwise excessive, not adequate or not relevant.[107] He concludes that the burden on employers of filtering comments against these rules might "de facto prohibit the use of customers' assessments".[108] In *Mevaluate*, the Italian Regulator went further, finding such practice legally – not just practically – impermissible.[109] Entanglement highlights the gap between the purposes for which data are collected from customers and applied to workers, suggesting ways this gap might be reduced to make the use of feedback more appropriate and practical. One option is to move the worker's purpose and process closer to the customer's

[105] Ibid.
[106] Todolí-Signes (n 3) 80.
[107] Ibid 80-81.
[108] Ibid 81.
[109] Ibid 76.

informal feedback by letting the worker select which comments to present in support of their performance assessment. Building on *Spikmich*, where teachers' ability to exclude comments helped to make the public discussion purpose acceptable, a worker's active selection of a portfolio of comments might be acceptable even for employee evaluation. Alternatively, formal 'feedback' might be gathered from a process in which the customer has a contractual, rather than consented, involvement. For example, the customer component of a worker's assessment could be based on how much repeat business they attract. Some customers may still make choices for arbitrary, irrelevant, or discriminatory reasons but when the choice directly affects them there is at least an incentive to be truthful. In each case an entangled perspective encourages a "data governance approach, … where companies thoughtfully design business strategy to use data responsively and parsimoniously", as recommended by Hoofnagel et al.[110]

Costello considers genetic data, which may contain sensitive health information about both the individual donor of the DNA sample and an unknown number of their ancestors, relatives, and descendants. She highlights many issues with using consent to process relatives' data outside formal health contexts: how can consent be obtained from those who are absent or not yet born; are distant relatives entitled to prevent processing by refusing consent; which relatives would have interest and standing to enforce their rights; and what sanctions are appropriate for a privacy breach caused by an individual donor's action. Indeed Bradford et al highlight that, even in national pandemic contact-tracing systems, consent – relying on a person "individually setting boundaries as to what organizations can and cannot collect and for what purposes" – is

[110] Chris Jay Hoofnagel, Bart van der Sloot, and Frederik Zuiderveen Borgesius 'The European Union general data protection regulation: what it is and what it means' (2019) 28(1) Information & Communications Technology Law 65, 76.

inadvisable where "an individual is poorly informed, or for one reason or another is not a rational or fair decision-maker".[111] An entangled approach to accountability stresses that it is the duty of the data controller, not the donor, to address these issues, and suggests ways this could be done.

First, entanglement confirms that a separate lawful basis is needed to process relatives' data: the donor's consent is not sufficient. As with worker feedback, entanglement favours lawful bases for donor and relatives that can be aligned, with voluntary limits on processing or additional safeguards to increase the area of overlap. Choosing a "necessary for…" basis for both groups of data subjects is a good start. Where the donor engages with a commercial service provider, at least some processing is objectively necessary to deliver the contracted service (Article 6(1)(b)).[112] The unavoidable processing of relatives' personal data might then be necessary for an Article 6(1)(f) legitimate interest of the provider. This requires safeguards to minimise the impact on individuals: the Article 29 Working Party identified commercial interests as "legitimate, but not particularly compelling" so only if the residual risk to relatives' (and donor's) interests, rights and freedoms is "even more trivial" can the processing take place.[113] In any case, the UK Information Commissioner considers that "invisible processing" of relatives' special category data would require a full Data Protection Impact Assessment (DPIA) not just a Legitimate Interests Assessment

---

[111] Laura Bradford, Mateo Aboy, and Kathleen Liddell, 'COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes' (2020) 7(1) Journal of Law and the Biosciences 1, 12.
European Data Protection Board, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' (8 October 2019), [30] <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf> accessed 10 June 2023.

[113] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controllers under Article 7 of Directive 95/46/EC' (9 April 2014), 31 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 10 June 2023.

(LIA).[114] Any additional retention or dissemination of personal data – including to relatives – must also serve a Legitimate Interest and satisfy a DPIA. Genetic data is one of the GDPR special categories so processing also requires a separate lawful basis from Article 9 though this "do[es] not have to be linked" to the chosen Article 6 basis.[115] Outside medical contexts explicit consent (Article 9(2)(a)) may be the only option. With processing and safeguards already designed to satisfy entangled "necessary for…" lawful bases under Article 6 this explicit informed consent provides an additional safeguard, not an exemption, to the data controller's duty to protect donor and relatives.[116]

An entangled principles analysis also responds to Costello's concerns about enforcement against[117] and by[118] individuals. Compliance with the GDPR – notably Articles 5, 6 and 9 – is the responsibility of the service provider, as data controller, not the donor. In particular, as discussed above, the security principle requires organisations that encourage the disclosure of entangled personal data to ensure these disclosures do not cause harm. Every data subject has the right to complain to a regulator but this is not necessary: regulators can investigate on their own initiative and enforce compliance directly including by ordering the termination of unlawful processing and imposing "effective, proportionate and dissuasive" financial penalties.[119] Though entanglement is still based in

---

114 Information Commissioner's Office, 'Data Protection Impact Assessments' (1 January 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> accessed 10 June 2023.

115 Information Commissioner's Office, 'Special Category Data' (1 January 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/> accessed 10 June 2023.

116 Bradford et al (n 111) 14.

117 Costello (n 33) 23.

118 Ibid 22.

119 GDPR, Chapter VIII.

"language that views group concerns as reducible to violations of individual protections"[120] its consequences do move towards Costello's preferred "relational model" that treats "members of the relational group as identified data subjects",[121] "captures the harms to non-consenting members of a … group",[122] and provides a "new framework for how we structure and think about consent and the uses and processes to which particularly sensitive data, such as genetic data, can be put".[123] Enforcing entangled principles could fill a gap, which Costello traces back forty years to the Council of Europe Convention 108, whereby laws recognise the possibility that harm may extend beyond the individual but do not offer any "means by which these group privacy impacts can be assuaged or addressed".[124]

6 Conclusion

This paper suggests that where the same personal data relate to multiple individuals new insights can be obtained by considering their data protection rights simultaneously. Simply raising this possibility may identify additional parties – in situations such as communications or correlated data – whose interests need to be considered. By highlighting the similarity or difference between how data protection principles, lawful bases, purposes, and rights apply to two or more groups this entanglement approach can help to foresee problems and – by indicating how changes to processing or voluntary safeguards could reduce any gaps – may suggest ways they might be mitigated. Problems are least likely where an overlap exists, or can be created, between the entangled

120 Costello (n 33) 7.
121 Ibid 23.
122 Ibid 13.
123 Ibid 22.
124 Ibid 11.

requirements, and where processing is (self-)constrained to remain within that common space. Several different types of data have been used to illustrate the approach: including comments, opinions, feedback, and DNA. The outcomes of three legal cases can be anticipated simply by identifying the entangled lawful bases involved: in *Nowak* both sitting a professional exam and marking it were necessary in the public interest, creating a large common area of acceptable processing; in *Spikmich* additional voluntary controls and safeguards were sufficient to reduce the distance between consented pupil comments on teachers and the public interest in discussing them; in *Mevaluate* the gap between consent and necessary for contract was too large to be fair and the regulator could find no suitable remedy. Considering entangled principles, lawful bases, purposes and individual rights confirms the concerns raised in three studies of opinions, feedback, and genetic data; but also suggests how altering data sources, processing and safeguards could make these activities safer, more effective, and better aligned with the requirements of data protection law. As Bradford et al highlight, "somewhat counter-intuitively, the GDPR's expansive scope is not a hindrance but rather an advantage in conditions of uncertainty":[125] an entangled analysis can help controllers explore the full range of potential solutions to novel situations. Hoofnagel et al suggest this could even "enable [processing] previously impossible under less-protective approaches".[126]

Finally, by shifting the focus from individual data subjects to data controllers, entanglement clarifies responsibility and provides more effective enforcement for harms that may affect networks of individuals.[127] The Article 5(2) accountability principle requires data controllers to take proactive measures to

[125] Bradford et al (n 111) 2.
[126] Hoofnagel et al (n 110) 65.
[127] Costello (n 33) 17.

meet the requirements of the Article 5 principles, Article 6 lawful bases, and Chapter III individual rights. For some entangled purposes this will be impossible: these combinations of data, purpose and impact are fundamentally unsafe. For others, aligning requirements may be more or less challenging. Where data controllers fail to practise and demonstrate accountability, regulators can order changes or impose "effective, proportionate and dissuasive" sanctions.[128] Unlike a tort or damages claim there is no need for an individual claimant to bring an action and sanctions are not limited to the actual harm caused. Regulators must "monitor relevant developments … in particular the development of information and communication technologies and commercial practices"[129] whether proposed (as in *Mevaluate*) or existing, as in the recent Belgian ruling on real-time bidding (RTB) for targeted adverts.[130] An observation in this latter case appears particularly relevant to data, such as DNA, that entangles the interests of many individuals. The Belgian Regulator contemplates that some processing might involve more parties than a data subject can reasonably read, for valid consent (para 435) or expect, for an interest to be legitimate (para 459). In that case the excessive list is of parties receiving personal data through the RTB ecosystem but the same concern might well apply to other large groups: relatives and descendants potentially impacted by processing genetic data; customers whose feedback affects workers; or friends used in making behavioural inferences. Processing that is designed to entangle only a

---

128 GDPR, Article 84(1).

129 GDPR, Article 57(1)(i).

130 Autorité de protection des données, Litigation Chamber, 'Decision on the merits 21/2022 of 2 February 2022: Case number DOS-2019-01377: Complaint relating to Transparency and Consent Framework', [435] <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022-english.pdf> accessed 10 June 2023.

reasonable number of individuals will be better placed to respond to any future development of this idea by regulators or legislators.