Of Men and Mice: Should the EU Data Protection Authorities’ Reaction to Google’s New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?

Judith Rauhofer*

On 24 January 2012, Google publicly announced the consolidation of its existing privacy policies covering over 60 of its different services into one main privacy policy1. The changes were presented as an effort to “integrate [its] different products more closely so that [it] can create a beautifully simple, intuitive user experience across Google” as well as a reaction to feedback from global regulators, which had been calling for shorter, simpler privacy policies. The new policy was due to come into effect on 1 March 2012.

Google’s announcement sparked an almost immediate reaction from EU data protection regulators concerned what the changes could mean for internet users given Google’s dominance within the EU not only of the market in online search but also in other online sectors. On 2 February 2012, the EU’s Article 29 Working Party wrote to Google asking it to delay the changes until the data protection implications could be checked2. It argued that “given the wide range of services [Google] offer[s], and popularity of these services, changes in [its] privacy policy may affect many citizens in most or all of the EU member states”. The Working Party also informed Google that it had asked the French data protection authority, the Commission Nationale de l’Informatique and de Liberté (CNIL), to take the lead in reviewing the compliance of Google’s new policy with the EU data protection framework.

Google refused to delay the introduction of the new policy, arguing that it had extensively pre-briefed EU data protection authorities on the changes prior to notifying them to Google account users, and had not been told by any EU regulator that any sort of pause would be appropriate3. However, on 27 February 2012, the CNIL4 wrote to Google confirming that after a preliminary investigation it had come to the conclusion that the new policy did not meet the requirements of the Data Protection Directive5. It criticized Google for consulting some EU data protection regulators but not others and for failing to give even those regulators that it consulted the opportunity to provide constructive feedback. Like the Working Party before it, it called on Google to delay the implementation of the new policy until it had completed its full analysis. However, Google refused this request and the new policy came into force on 1 March 2012 as previously announced.

In its letter to Google, the CNIL had raised particular concern about the lack of transparency on Google’s part about its processing activities and Google’s claims that it will combine data across services. Although, the new policy did not specify whether or not this right to combine information also applied to data already held by Google services before the new policy came into force, it can be assumed that this was Google’s intention.

Under Article 6(4)(b) of the Data Protection Directive personal data can only be “collected for specified, explicit and legitimate purposes and not fur-

---

* Judith Rauhofer is Lecturer in IT Law, University of Edinburgh; Judith.Rauhofer@ed.ac.uk.
5 95/46/EC.
ther processed in a way incompatible with those purposes” (purpose limitation principle). In practice, a combination of existing data about a single user from a variety of previously unconnected sources for uses that may not have been envisaged at the time at which that data was collected could therefore lead to a failure by Google to comply with that requirement.

This question is important given Google’s dominant position in the online market place as the potentially biggest personal data broker on the global stage. In the online environment, the commercial exploitation of personal data has become one of the leading revenue generation strategies for online providers. The use of personal information to profile internet users for their preferences and shopping habits and the sale of that data to third parties for that purpose has already turned personal information into a commercial asset of significant economic value. Big Data, i.e. the cost-effective, innovative form of processing vast amounts of data from different sources at near real time speed for enhanced insight and decision-making, is now further changing businesses’ view about the way in which they should be able to use the information they hold about their users in new and creative ways. The business models espoused by Google are likely to influence the approach of other online providers and many eyes will be focused on the way in which and the extent to which EU regulators manage to defend the Union’s data protection principles against pressures from the digital market place.

This article will explore whether or not Google’s new privacy policy complies with the purpose limitation principle and the way in which EU data protection authorities have reacted to its implementation at EU and national level at a time when the EU data protection framework as a whole is under review.

I. Pushing the Big Data envelope: Google’s new privacy policy

Google’s new privacy policy applies “to all of the services offered by Google Inc. and its affiliates”, including services offered on other sites (such as its advertising services), but excluding services that continue to have separate privacy policies. It also applies to some services like Chrome, Google Books and Wal-

let that, although they incorporate the new policy, also use top-up provisions describing the privacy practices that are specific to their service.

Among other things, the new policy introduced changes to the description of the types of information Google collects about its users, the way in which it uses the information it collects, and Google’s transparency and choice mechanisms.

1. Types of information collected

The description of the type of information collected by Google now specifically distinguishes between information it obtains from internet users’ use of its services (including device information, log information, location information, local storage information and information gained from cookies and other anonymous identifiers) and information provided to Google by users themselves when they sign up for a Google account. In practice, the new policy therefore applies equally to users who use at least some Google services by identifying themselves to Google (and who are encouraged to create a publicly visible “Google profile”) and incidental users who use Google services on an anonymous basis.

The new policy’s description of the information Google collects became slightly more detailed and acknowledges new ways of data collection (for example, device information, local storage and anonymous identifiers other than cookies). The new policy therefore arguably improved Google’s transparency about its data collection practices.

2. Transparency and choice mechanisms

Under its previous privacy policy Google referred users to Google Dashboard for reviewing and con-

---


trolling the information stored in their Google account. It also explained how to reset a browser to refuse all cookies and how to manage ad preferences by using Google’s Ads Preferences Manager. The new privacy policy still mentions those two user tools although it now makes clear that Dashboard can only be used to review “certain types of information” tied to a user’s Google account. Specific user control tools that allow a user to see and adjust how their Google Profile appears to particular individuals and to determine who they share their information with are also highlighted for users with a Google+ profile. Finally, a new data management tool now allows users download their data in an “open, interoperable, portable format”.

However, there is no means for users without a Google account or Google profile to control the uses Google makes of the information it obtains about them and their online behavior through the use of cookies and other tracking devices. Although much of this information may not be considered personal data in the context of the EU data protection framework since it does not identify a particular user, this still allows Google to use that information to “single out” particular users by tailoring their search results and the content they may be offered as well as target the ads they are shown.

3. Information uses and combining information

Under the new privacy policy, the purposes for which Google uses the information it collects became considerably more general compared to the previous policy. Although that policy included a general catch-all provision that allowed Google to use user data to “provide, maintain, protect, and improve [its] services (including advertising services) and develop new services” and to “protect the rights or property of Google or [its] users” it had also provided specific information on the purposes for which some of the distinct categories of data that Google collects would be used.

For example, while the old policy informed users that cookies would be used for “storing user preferences, improving search results and ad selection, and tracking user trends, such as how people search” the new policy simply describes cookies as a means to “enhance the user experience and the overall quality of [its] services”. At the same time, the new policy now applies purposes that were previously limited to cookie data (tailoring content, improving search results and targeting ads) to all other data it collects, thus potentially expanding the extent to which Google is permitted to use that other data.

The new policy also grants Google the right to “combine personal information from one service with information, including personal information, from other Google services”. While the old privacy policy already permitted Google the right to combine information with information from other Google services or third parties, this was limited to information a user submitted under their account and did not apply to other information collected by Google like cookie data, location data or log information. Unlike the old privacy policy, the new policy does not give users the right to opt-out of combining such information for certain services.

In practice, the changes meant that Google would be able to aggregate users’ personal data from across almost all of their accounts and services including Gmail, Google Play, Google+, internet searching, Google Map, Youtube etc. to create a highly personalized profile that it could then use for very general purposes, namely to “provide, maintain, protect and improve [its services], to develop new ones, and to protect Google and [its] users”.

In the context of the EU data protection framework, this raises two questions. One, it must be asked whether such a widely construed purpose is sufficiently specific to allow users to gain an understanding of the uses Google makes of their personal data; and two, whether the combination of existing data already held by Google at the time the new privacy policy came into force can be justified on this basis given that users would not have been aware at that time, that such further processing of their data might take place. To answer these questions it is necessary.

---

10 See supra, note 8, “Information we collect and how we use it”.
11 See supra, note 7, “How we use information we collect”.
12 See supra, note 8, “Information we collect and how we use it”.
13 See supra, note 7, “How we use information we collect”.
to explore the scope of the purpose limitation principles contained in Article 6(1)(b) of the Data Protection Directive.

II. Purpose limitation in EU data protection law

Article 6(1)(b) provides that personal data must be collected for specified, explicit and legitimate purposes, and not be further processed in a way incompatible with those purposes. The principle is an expression of the fundamental right to privacy set out in Article 8 of the European Convention on Human Rights (ECHR) and Article 7 of the EU Charter of Fundamental Rights (EU Charter). It could be argued that it intended to safeguard individuals’ right to informational self-determination, i.e. the right to control who has the right to process information about them and for what purpose. It sets limits on how data controllers can use a data subject’s personal data once it has been collected, thereby preventing uses that data subjects may find unexpected, inappropriate or otherwise objectionable.

1. Purpose specification

To comply with the purpose limitation principle, the data controller must clearly and specifically identify the purpose “at the time of collection of the data”. The data controller must also notify the purpose to the data subject as part of his fair processing obligations, for example, in its privacy policy.

In its 2013 opinion on purpose limitation, the EU’s Article 29 Working Party explains that a specified purpose must be detailed enough to allow the data subject to determine what kind of processing is and is not included within it. The Working Party states that data controllers should avoid purposes that are vague or too general. It suggests that purposes like “improving user experience”, “marketing”, “IT security”, and “future research” would not usually meet the criteria of being “specific”. The degree of detail to which a data controller should specify a purpose depends on the particular context in which the data are collected and the type of personal data involved. While in some cases simple language may be sufficient to provide appropriate specification, in other cases more detail may be required.

Although data controllers may collect personal data for a number of different related or unrelated purposes, they should avoid specifying overly broad purposes with the sole intention of justifying various further processing activities that may only be remotely related to the initial purpose. This is particularly the case, where such further processing activities are possibly not even anticipated at the time the data are collected. Ultimately, each purpose must be specific enough to allow an objective assessment of whether the processing of the data for the stated purposes complies with the law and to establish which safeguards should apply. According to the Working Party’s opinion, “sufficient granularity will be needed to make sure that all the different purposes are sufficiently clear for the users.”

The purpose must also be explicit. According to the Working Party, this means that it must be clearly revealed, explained or expressed. In particular, the data controller must communicate the purpose in a way that creates an “unambiguous understanding of the purposes of the processing irrespective of any cultural or linguistic diversity.”

2. Compatible use

The way in which the personal data are processed must also be compatible with the purpose originally specified. Further processing of existing data for incompatible purposes is prohibited.

According to the Working Party, any processing of personal data after their initial collection constitutes further processing of that data and must meet the compatibility requirement. In its 2013 opinion, the Working Party sets out a number of criteria, which data controllers should take into account when assessing the compatibility of further processing oper-

---

15 Recital 28, Data Protection Directive.
16 Article 10(b), Data Protection Directive.
17 Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP 203), 2 April 2013.
18 Ibid., p. 15.
19 Ibid., p. 52.
20 Ibid.
21 Ibid., p. 51.
22 Ibid., p. 39.
23 Ibid., p. 21.
ations with the purpose originally specified. They include (1) the relationship between the purposes for which the data was originally collected and the purpose of further processing, (2) the context in which the data has been collected and the reasonable expectations of the data subject about their further use, (3) the nature of the data, (4) the impact of the further processing on the data subject, and (5) the safeguards applied by the data controller to ensure fair processing and to prevent any undue impact on the data subject.

According to the Working Party, a compatibility assessment must be a substantive rather than a merely formal exercise, meaning that that it should go beyond a mere formal comparison between the original purpose and the envisaged further use to find out whether that use is covered.

It could therefore be argued that even if the original specified purpose permits a data controller to process two distinct sets of personal data for the same or a similar purpose (for example, improving the user experience), this does not mean that this would also authorize the combination of those two data sets for that same purpose if the impact of that further processing on the user is significant, for instance, if the data is combined and processed with other data for profiling purposes.

III. The EU regulators’ reaction to Google’s new privacy policy

To facilitate the full investigation of Google’s policy, which it had started in February 2012 at the request of the Article 29 Working Party, the CNIL sent a letter to Google Inc. in March 2012, which contained a list of 69 questions on Google’s data processing activities. The questions covered the full range of privacy issues raised by the changes, including matters such as user consent, use of cookies and online behavioural advertising and the combination of users’ data collected via different Google services.

1. CNIL common findings and recommendations

The CNIL published its findings on behalf of the Working Party in October 2012. Among other things, the findings explore whether Google has complied with the information requirement set out in Articles 10 and 11 of the Directive and whether its combination of data across different services “respect the principles of proportionality, purpose limitation, data minimization and right to object.”

a. Compliance with information requirement

Faced with a limited number of very widely phrased purposes contained in the new privacy policy, the CNIL had to decide whether this constituted a breach of the purpose limitation principle set out in Article 6(1)(b) of the Directive (because the purposes are not sufficiently specified and expressed) or of the fair information requirements set out in Article 10 and 11 (because Google processes personal data for additional specific purposes that it did not describe in the privacy policy).

In this case, the findings confirm a breach of the fair information requirement as the new privacy policy provides only incomplete or broad information about the categories of data the individual Google services process, the extent of Google’s actual processing activities, and the purposes for which individual services process personal data. The findings particularly criticize Google’s failure to provide specific information to users about what data is combined between which services.

The document recommends that the information provided to users must describe the purposes and categories of data processed in a clear and accurate manner, detailing for each processing the exact purposes and data collected (including data from other services). The processing operation itself must be conducted with due respect to the rules of propor-
tionality and data minimisation, which must be reflected in the information that is delivered.

Notices about each processing activity must not be modified unless the user has given his consent, having been provided with clear and comprehensive information inter alia about the changes to be implemented. In addition, notices should be traceable33. Similarly, Google is asked to make sure passive users, i.e. users without a Google account but where Google nonetheless collects information about their use of Google services, are correctly informed about the processing operations that concern them34.

b. Combining of data across services

The document also criticises Google for the way in which its combination of data fails to respect the principles of proportionality, purpose limitation, data minimization and the right to object15. The findings identify a total of eight different purposes for the combination of data across Google services. It found that “Google does not differentiate the different purposes for the combination of data and does not clearly endorse the principle of purpose limitation”36.

The document also examined the lawfulness of the combination of data, in particular, whether the processing for each of the purposes is justified by one of the legal grounds set out in Article 7 of the Directive. It concluded that only four of the purposes were based in one of those legal grounds. The processing of user data for any of the other four purposes – the provision of services requested by the user where the combination of data applies without the user’s knowledge (search result personalization), marketing innovation and product development, advertising purposes and analytics purposes – were carried out without a legal basis. In particular, Google could not rely on the users’ consent37 in those cases as the limited information provided to users in the privacy policy meant that they were not aware of the exact extent of the combination of data38. Google could also not rely on the legitimate interest condition set out in Article 7(f) of the Directive, since Google’s interests to implement the extensive combination of data were overridden by the interests for fundamental rights and freedoms of the data subject39.

The Working Party therefore recommends that where the combination of data requires a legal basis, Google should adopt a privacy-by-design approach (anonymisation, simple opt-outs and retention periods)40. In respect of the four purposes for which personal data was at the time processed with a legal basis, Google was advised to seek the explicit consent of their users and make opt-out mechanisms available in one place41. In addition, the Working Party advises Google to develop new tools to allow users to control, which services may combine data42.

c. Evaluation

While the document’s criticism of Google’s lack of transparency is certainly justified, its failure to emphasize Google’s failure to comply with the purpose limitation principle is regrettable. Although the document acknowledges that the purposes for which Google may combine user data across services are not sufficiently expressed and specified, the document’s focus in this regard is on the failure to comply with the fair information requirement set out in Articles 10 and 11 of the Directive. This pulls focus from the separate requirement under Article 6(1)(b) and the fact that there is more at stake than just transparency about the nature of Google’s processing.

In particular, the document does not examine whether the combination of data constitutes an act of “further processing” at least with regard to existing data Google already held at the time the new policy came into force. This is arguably the case, which means that Google should have been required to carry out a specific compatibility assessment with regard to each combination of data to establish whether it is compatible with the purpose for which the data

33 Ibid.
34 Ibid.
35 Ibid., p. 4.
36 Ibid.
37 Article 7(a), Data Protection Directive.
38 See supra, note 27, p. 4. In theory, this means that Google might be able to justify its processing in those cases by providing users with additional information about them. In the CNIL’s view, increased transparency might therefore result in making the combination of data lawful.
39 Ibid.
40 Ibid., p. 7.
41 Ibid.
42 Ibid., p. 8.
were originally collected taking into account the reasonable expectations of the data subject about, the impact of the further processing on the data subject, and the safeguards applied by Google.

That this did not happen is likely due to the fact that the Working Party’s Opinion on purpose limitation43, where those criteria were first developed in some detail, was only published more than a year after the CNIL’s investigation. It must therefore be examined whether subsequent actions of EU data protection regulators take those guidelines into account.

2. The Article 29 Working Party’s common list of measures

In September 2014, the Working Party itself followed up on the CNIL’s initial analysis by sending a letter to Google reminding it of its ongoing obligation to comply with the EU data protection regime44. Attached to the letter were guidelines containing a common list of measures for amending its privacy policy that Google was encouraged to implement45. The Working Party also confirmed that it might publish further guidance on specific issues to the entire industry at a later stage thereby highlighting the test case nature of its dispute with Google.

Among other things, the common list of measures includes suggestions for Google to ensure that the information it provides to users is accurate and comprehensive46. The Working Party reiterates that the privacy policy must be structured so as to provide clear, unambiguous and comprehensive information regarding the data processing, including an exhaustive list of the types of personal data processed by Google, and all the purposes for which those data are processed47. As a general rule it should enable users to have, on a single page, a comprehensive picture of the personal data processed by Google and for which purposes. It must also present important new purposes for its processing activities in its privacy policy and not in its terms of service. The policy should avoid indistinct language such as “we may...” and using, for example, “if you used services A and B, we will ...”. In addition, the Working Party reminds Google that it must obtain user consent prior to processing.

Unlike the original findings and recommendations document produced by the CNIL, the list of measures does not address the question whether Google has the right lawfully to combine data across different services or whether the particular combination of data envisaged by Google complies with the purpose limitation principle.

Similarly, like the findings and recommendations document, the Working Party’s common list of measures does not distinguish between data already collected and stored by the various Google services at the time the new policy came into force and data those services collected afterwards. This means that the question of whether the combination of existing data as a “further processing activity” is compatible with the original purpose notified to users remains unanswered.

Instead the document focuses on increasing transparency and the deployment of user control tools. It can therefore be seen as a shift away from pre-emptive regulatory control of Google’s data processing activities by means of enforcement of the purpose limitation principle to a situation where the responsibility to ensure that Google complies with that principles is given to users themselves via an improved ability to understand Google’s processing activities and to control the way in which and the extent to which their personal data is processed through “more elaborate tools to manage their personal data”48.

3. Consolidated action of national EU data protection authorities

In April 2013, and after Google had failed to amend its privacy policy or implement any other significant compliance measures in response to the CNIL’s findings and recommendations, six data protection au-

---

43 See supra, note 17.
46 ibid., “Information”.
47 ibid.
48 ibid., “User controls”.
authorities from France, Germany, Italy, the Netherlands, Spain and the UK announced that they would take consolidated action against Google to examine whether its privacy policy complies with their respective national data protection legislation. To this end, they initiated an inspection procedure in April 2013 and set up an international administrative co-operation procedure.

a. Spain and France

Spain was the first to conclude its investigations in December 2013 when it found Google in breach of Spanish data protection laws and fined it the maximum fine of €900,000. The CNIL in France quickly followed suit in January 2014 with a fine of €150,000, while the authorities in the other four countries took steps to force Google to make significant changes to its privacy policy.

b. Italy

In July 2014, the Italian data protection commissioner gave Google 18 months to change the way it processes and stores users’ personal data. In particular, it stated that Google must obtain users’ consent to use personal data and make it clear that this data may be used for commercial profiling. Google was asked to present a detailed plan of the concrete steps it intended to take by September 2014.

c. Germany

In September 2014, the data protection authority of the German state of Hamburg issued an administrative order against Google, which requires Google to collect and combine user data only in accordance with the existing German data protection framework. In particular, the order noted that the practice of user profiling affects the privacy of Google users far beyond the admissible degree. Google was ordered to take the necessary technical and organizational measures to guarantee that their users can decide on their own if and to what extent their data is used for profiling.

d. The Netherlands

In December 2014, the Dutch data protection authority declared that Google was in breach of Dutch data protection laws. It ordered the company to change its data processing activities by the end of February 2015 or face a fine of up to €15 million. The authority found that Google’s combining of personal data under its new privacy policy is in breach of the Dutch data protection act and that Google does not properly inform users which personal data the company collects and combines, and for what purposes. The authority noted that Google does not offer users any (prior) options to consent to or reject the relevant data processing activities. It also made it clear that the consent, required by law, for the combining of personal data from different Google services cannot be obtained by accepting general (privacy) terms of service but that it must be informed and specific to the relevant processing activity and purpose.

In particular, the Dutch regulator ordered that Google must ask for the unambiguous consent of users for the combining of personal data from the different Google services. It suggested that this could be achieved via a separate consent screen.

The authority also requested Google to further clarify the information in its privacy policy in order to provide clear and consistent information to people on which personal data are used by the different services of Google.

e. The United Kingdom

As the last of the six data protection authorities, the UK’s Information Commissioner’s Office announced in January 2015 that Google had agreed to sign a formal undertaking to improve the information it provides to people about how it collects personal data in the UK.\(^{55}\) The undertaking was preceded by lengthy negotiations between Google and the ICO after the ICO’s own initial investigation had concluded that the search engine was too vague when describing how it uses personal data gathered from its web services and products.

As part of those negotiations, Google had initially proposed a number of measures designed to address the ICO’s main concerns with a view to implementing them by the end of June 2014.\(^ {56}\) Unlike the findings and recommendations and the requirements set out by some of the other EU data protection authorities, the suggested measures largely focused on improving transparency and the information Google provides to its users. Among other things, Google proposed to change the privacy policy and provide further notice to users by (1) developing an overlay to the privacy policy which would include clarifying examples to illustrate what the text of the Policy means in practice, (2) providing a new section within the privacy policy with additional relevant information, including information about its use of cookies, (3) providing additional explanations of technical terms, (4) providing increased notice, information and help for passive users, and (5) simplify, enhance and unify general user privacy controls.

The Information Commissioner agreed that the measures would address his concerns as long as sufficient information was provided to users, and this information was easily accessible.\(^ {57}\) Unlike most of his EU counterparts, the Commissioner also decided that in the light of Google’s implementation of the proposed measures in accordance with the agreed timetable, formal regulatory action in the form of an enforcement notice\(^ {58}\) was both inappropriate and unnecessary.

However, the Commissioner believed that Google could still make further improvements. Consequently, Google’s formal undertaking was given under section 40 of the DPA.

Among other things, Google undertakes to (1) ensure the continued evaluation of the privacy impact of future changes to processing which might not be within the reasonable expectations of service users, (2) keep the content of its privacy policy and associated web content under review and take appropriate actions so that service users are informed as to the ways in which their personal data may be processed, (3) ensure that any significant future changes to its privacy policy are reviewed by user experience specialists and with representative user groups before the policy and associated tools are launched as appropriate, and (4) continue to pro-actively cooperate with the Commissioner and provide appropriate advance notice of any significant changes.\(^ {59}\)

Google has also agreed to comply with a number of enhanced information requirements.\(^ {60}\) Among other things, Google must enhance the accessibility of its privacy policy, describe its data processing activities more clearly (including the types and purposes for which it processes user information), and launch a redesigned version of its account settings, which would allow users to find a variety of privacy controls and information more easily. The requirements by and large are phrased widely, thereby giving Google significant discretion in deciding how to comply with them. This is in contrast with the much more specific demands set out in the Article 29 Working Party’s 2013 findings and recommendations and its 2014 common list of measures. Google is currently given until August 2015 to provide a report to the ICO setting out the steps it has taken in response to the commitments set out in the undertaking.

Compared to the actions of other EU regulators, it is clear that the ICO’s response has been less confrontational and more collaborative. This is in line with the general approach to enforcement the ICO has adopted in recent years, where businesses are often offered time and support in their endeavor to achieve compliance with the DPA. To date the ICO has only made limited use of its enforcement powers (including its powers to impose monetary penalties) outside the areas of blagging, nuisance communications and data security breaches. The approach


\(^ {56}\) Ibid., p. 4.

\(^ {57}\) Ibid., p. 5.

\(^ {58}\) Section 40, Data Protection Act 1998 (DPA).

\(^ {59}\) See supra, note 55, p. 6.

\(^ {60}\) See supra, note 55, Annex 1.
in this case is therefore unsurprising even while it is disappointing.

Since it introduced its new privacy policy on 1 March 2012, Google has made six further revisions to it\(^\text{61}\). Until now, most of the revisions were minor although Google did gradually begin to add more information about technical terms in the form of overlays. To date, none of the changes to the policy have substantively changes Google’s right to combine personal data across services. It remains to be seen whether this will change as Google nears the various deadlines set by some of the national data protection authorities.

IV. Conclusion

Given the complexity of Google’s data processing activities, the vast amount of data it processes about almost every EU citizen and the reliance of many internet users on its services for both their personal and professional activities, it is at least questionable, whether the EU and most of the national regulators’ recent steps to reign in Google’s plans to combine data across different services are sufficient to protect internet users from the potential negative consequences of that type of processing of their personal data without sufficient safeguards and limitations.

While the Working Party’s 2013 findings and recommendations were clear that any combination of data requires a legal basis and, in some cases explicit user consent, much of the subsequent regulatory action by national data protection authorities does not seem to have focused on this point. Most of the regulators have also largely ignored the question whether the combination of data across different Google services complies with the purpose limitation principle. In the age of Big Data, this is an important concession for online providers whose business model is based on their ability to profile their user base with a view to targeting advertising, goods and services.

At the same time, this approach shifts the responsibility for controlling the way in which their data is processed to the internet users themselves, who, in many cases, may have neither the skill nor the bargaining power to resist commercial demands for their data. Academic scholars have long criticized the overreliance of EU data protection law on user consent in a situation where those users are faced with a choice either to provide their data to online providers or to lose out on the ability to use those providers’ services\(^\text{62}\). Calls have therefore been made for a framework that imposes limits on certain data processing activities in the same way in which consumer protection law restricts other commercial activities.

Despite the Article 29 Working Party’s and most of the national regulators’ expectation that Google should provide users with more information about the purposes for which it combines their data, the fact remains that the majority of algorithms Google uses to, for example, personalize search results, tailor content and target advertising, are closely guarded trade secrets, a black box to which the average user does not have access\(^\text{63}\). This makes it difficult for users to understand what exactly Google does with their data, much less protect themselves from the potential unwanted consequences of Google’s data processing activities. However, if one partner to a commercial transaction is able to create increasingly accurate profiles of the other’s online behavior, preferences and social status to the extent that this allows it to predict the other partner’s likely reactions, this creates an uneven playing field that further disadvantages individuals in their capacity as consumers of online content and services.

In this particular case, the knowledge imbalance that the right to combine personal data from a variety of different sources creates between Google and its users – i.e. the difference between what Google knows about its users’ activities compared to what users know about Google’s activities – is starkly representative of much that is questionable about Big Data technologies. Among other things, that imbal-


\(^{63}\) Some of the long-term potential harms of life in the new “black box society” are comprehensively addressed in Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information, 2015, Harvard University Press.
ance could ultimately result in (1) discrimination of individual users both with regard to the price they pay for goods and services and the extent to which they will be allowed access to those goods and services in the first place; (2) social categorization and stigmatization; and (3) self-imposed filter bubbles based on previously accessed online content of which users will likely be largely unaware despite the fact that they have unwittingly assisted their creation. The impact that, in particular, such filter bubbles may have on societal discourse if individuals begin to live in a separate world of their own choosing without ever being exposed to uncomfortable outside influences cannot yet be fully assessed.

Furthermore, the potential for power abuse and the potential impact on individuals’ personal autonomy that is inherent in this situation is arguably significant enough that it would warrant, at the very least, some kind of regulatory intervention, if only in the form of a robust enforcement of the purpose limitation principle that still forms one of the fundamental elements of the current EU data protection regime. However, as this article has shown, this is not currently the case at EU or national level.

Instead Google has managed skillfully to re-direct the discussion about its new privacy policy from one that was genuinely concerned with the question whether Google should be permitted to combine user data across different services to one where this right to combine data is taken as a given provided that it is done in a transparent manner. At the very least to the extent that this is also accepted for existing user data, this approach completely undermines one of the central components of the purpose limitation principle, namely the prohibition on further incompatible processing.

Despite the fact that the Working Party has issued a comprehensive opinion on that principle just over two years ago, it and the national regulators that make up its constituency have so far shied away from taking decisive steps towards its enforcement. In the light of market pressures to loosen the regulatory framework in the age of Big Data and given the ongoing revision of the EU data protection framework and the numerous attacks on the essence of that principle from industry and even some EU member states, this is a worrying development that should be kept under close review.