Internet Policy Review
13 June 2019

Data subjects as data controllers: a Fashion(able) concept?

Lilian Edwards, *Newcastle University, UK*
Michèle Finck, *Max Planck Institute for Innovation and Competition, Munich, DE*
Michael Veale, *the Alan Turing Institute, UK*
Nicolo Zingales, *University of Leeds, UK*

Internet Policy Review, 13 June 2019, at https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400

Introduction

Recent case-law of the European Court of Justice has substantially widened the notion of “data controller" in unclear and potentially onerous ways for a range of actors involved in personal data processing. While this approach may be positive for data protection compliance generally (generating a ‘ripple effect’, in the words of late Advocate General Bot), it also has worrying implications for data subjects who may be characterised as controllers, and for emergent decentralised and privacy protective technologies; we hope the Court will address these issues in its forthcoming judgment in Case C-40/17, *Fashion ID*.

The expanding notion of data controller

The European Union’s General Data Protection Regulation (‘GDPR’) recognises two main categories of actors: data subjects and data controllers. Pursuant to Article 4(1) GDPR, the data subject is the identified or identifiable natural person that personal data relates to. The data controller is the entity that ‘alone or jointly with others, determines the purposes and means of the processing of personal data’ (Article 4(7) GDPR). Whereas the Regulation implicitly assumes that data controllers and data subjects are different actors, recent technical and legal developments have made the dividing line between both sets of actors less clear-cut. Increasingly, users may find themselves deemed to be acting as joint controllers with service providers, or even as sole controllers. This qualification matters, because effectively it places the principal, onerous duties in the data protection regime on the users themselves, which may be inappropriate for legal and technical reasons, as well as prejudicing the rights of (other) data subjects. After a period of turmoil in the case law, helpfully the European Court of Justice (ECJ) will have a chance to review this area of law again in the upcoming *Fashion ID* case, which has already generated a controversial Opinion by AG Bobek[1], with a final judgment expected before the Court’s 2019 summer break in mid-July.

When the foundations of EU data protection law were being laid, typically one entity controlled both the means (the ‘how’) and the purposes (the ‘why’) of processing (think of census data processed by public authorities, or payroll records kept in a company). Data crunching itself was often outsourced to a third party, but their subordinate role as data processor was usually clearly delineated in the contract made with the controller company. Nowadays, however, data ecosystems are often much more complex, with the consequence that there is no unitary control over the means *and* the purposes of processing. Furthermore, systems are increasingly distributed regarding infrastructure and organisation. Consider the example of cloud computing, where arguably providers determine the means but their clients determine the purposes of processing. Traditionally cloud providers have been seen as mere data processors but this no longer captures the diversity of business models, the ways in which they can shape data controllers' processing operations, and the intermingling of their own purposes with those of their clients. Similarly, where blockchain technology is used, oftentimes the purposes are determined by the users, but they have no influence over the means of processing, which are rather determined by the actor(s) that control the infrastructure (usually not users). This led the French Data Protection Authority to argue in its guidance on blockchains and the GDPR that a data subject could indeed be a data controller in relation to personal data that relates to themselves.

In a series of recent judgments, the ECJ has added to the confusion between data subjects and data controllers in adopting a very broad definition of the notion of controllership, striving to ensure the 'effective and complete protection of data subjects'. In *Wirtschaftsakademie Schleswig-Holstein*, the Grand Chamber decided that operators of a Facebook fan page were joint controllers together with Facebook, merely because they exerted influence over Facebook's collection of data from visitors to that page.[2] In the *Jehovah's Witnesses* case the court found that the Jehovah's Witnesses community was a joint controller (together with the individuals doing door-to-door preaching) of collected data as it organised, coordinated and encouraged such collection despite never gaining access to this data.[3] As Advocate General Bobek aptly noted in his opinion in *Fashion ID* taken to extremes this means that anyone in a "personal data chain" that makes data processing "possible", becomes a joint controller.[4]

Implications: limitations of 'everyone is a controller' approach

This tendency towards the *widening* of responsibility via joint controllership may be particularly perilous for consumers or domestic users seeking greater control over data through emerging privacy protective architectures known as *personal data stores* (PDSs). Here, instead of data being held and processed in a centralised manner on the cloud, it is retained in a decentralised manner by data subjects themselves. Privacy-preserving computations can then be used to generate inferences from t his data and thus provide users with services like price comparison or search without their data ever leaking to an external platform. In times of concern about the monetisation of user privacy and the rise of "surveillance capitalism",[5] such experiments are important. Using cryptographic systems built on tools like secure multi-party computation and homomorphic encryption, even centralised machine learning models can still be trained from this decentralised data.[6]

This raises a number of key problems for data protection regimes. First, data subjects using PDSs – especially perhaps in "smart homes" – are likely to be seen as joint controllers, but may also find no succor from the so-called “household exemption” which was designed to protect domestic users, such as those running club mailing lists, from the full rigours of controllership. Article 2 GDPR exempts from its scope data processing “by a natural person in the course of a purely personal or household activity”. This has been interpreted narrowly, as in *Lindqvist*,[7] but two additional criteria of judicial origin, namely that data must not be shared with an indefinite number of people and that processing must not be ‘directed outwards from the private setting of the person processing the data’, mean that the household exemption is very unlikely to protect smart home users who seek external services or, perhaps unintentionally, process the data of visitors to their home.[8] Secondly, data stores, similarly to distributed ledger technologies, may place data controllers in a contrary position as actors orchestrating or coordinating processing, but not actually seeing the data themselves. The ECJ has held that this does not prevent them acting as joint controllers: both *Wirtschaftsakademie* and the overarching *Jehovah’s Witnesses* organisation did not have copies of the data but were nonetheless seen as controllers.

In these decentralised set-ups, how effective is data protection law? Where there are joint centralised-controllers and data subject–controllers, how does responsibility fall? Will this lead to more cases where central data controllers bind their own hands as not to be able to exercise full data controller responsibilities, such as access or erasure?[9] What about cases with no discernable central, orchestrating body at all, as on public and permissionless blockchains? One way forward might be to look closer at the GDPR’s provisions around *data protection by design* (Article 25), ensuring that decentralised systems have safeguards baked in at their heart. However, it seems unlikely that even careful, concerted design could fully support a model where already over-burdened data subjects are expected to undertake controller obligations too.

Another approach, which is championed by Bobek in *Fashion ID*, would be to consider more carefully in *law* how joint controller responsibilities should be allocated, and for what stages of processing. Bobek’s own solution, however, which seeks to limit the spread of joint controllership by deeming two actors joint controllers *only* for the *stages* of processing where they determine *common* purposes of processing, may be hard to determine with any specificity and predictability. It may thus deprive data subjects of effective protection, in particular where they lack knowledge of the specific purposes of third party processing that they enable. Further, responsibility and potential liability of an ‘enabling controller’ in the absence of knowledge or awareness of illegality in the activity of its joint controller(s) appears to be in striking tension with the safe harbour established by article 14 of the e-Commerce Directive for content hosts.

Conclusion

Given the above, we submit that the apparent widening of responsibility of data subjects for the processing of their own data is a worrying trend which may impede both the development and uptake of privacy protective technologies that are badly needed, as well as decentralised data ecosystems that are being promoted as innovative by many EU member states. To avert those consequences, it is hoped that the Court will address some of the uncertainties and shortcomings in the existing doctrine of joint controllership. For these reasons, the *Fashion ID* judgement is one to watch with anticipation.

Funding declaration

Michael Veale was supported by The Alan Turing Institute under the EPSRC grant EP/N510129/1. Lilian Edwards was supported by EPSRC grant EP/S035362/1.

Footnotes/References

1. Case C-40/17 *Fashion ID* (Opinion of Advocate General Bobek) ECLI:EU:C:2018:1039

2. Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388.

3. Case C-25/17 *Tietosuojavaltuutettu* ECLI:EU:C:2018:551.

4. Supra n 3 at para 74.

5. Shoshana Zubhoff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs, 2019).

6. Royal Society (2019) Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis. https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/ .

7. Case C-101/01 *Lindqvist* (2003) EU:2003:596.

8. Case C-12/13 *František Ryneš v Úřad pro ochranu osobních údajů* EU:C:2014:2428, para 33.

9. Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law, 8*(2), 105-123.