

Transparency as translation in data protection

Gloria González Fuster*

Abstract

For unwitting individuals presumably lost amidst a profusion of unclear data processing practices in our data-driven societies, transparency seems to appear as the last great escape. Transparency could be, it sometimes seems, the great opportunity for “data subjects” to directly perceive -and comprehend- what happens for real to the data linked to them, and what might actually happen to them as a result of all the data processing that surrounds us. In data protection law, however, transparency is not an open door into the realities of data processing. Transparency, as a matter of fact, is rather about obliging data controllers to author a certain narrative of their own data practices, to be constructed on the basis of a certain idea of the data subjects they target. It is a transcription of an account that is conditioned by these premises, and cannot thus result in an unmediated image of what is actually going on. Transparency, therefore, is not a window into how individuals are being profiled, but a productive translating operation – and, thus, as such, a primary “being profiled”.

Keywords: transparency, translation, data protection, subject, GDPR

Introduction

‘Oh, I see’, said the data subject. And went on to add: ‘Yes, I do see why you are collecting all this information about me. I vividly visualize the data you are taking away from my hands. And I can nicely picture with whom you will share it – well, at least the type of people you might, and probably will, share it with. I am delighted now I actually know who you are. I will cherish your contact details while you process all these data, which shall however not be forever, as you somehow melancholically, but certainly accurately, have pointed out. I sincerely appreciate you are able to prove all this processing is lawful – that there is a legal ground, a good reason why this happens, and that, if there was none, all this might still be fine if I freely agree with it, on my own will. I welcome all your kind explanations about the line of reasoning behind the data-driven automatic decisions you will be taking about me sooner or later. They mean so much to me. And I am deeply touched by your efforts in describing how these decisions will make a real difference in my life. I am ecstatic hearing you talk about the existence of a series of rights I have, that I could maybe use. I can almost feel the presence of your data protection officer right here by my side’.

This is, perhaps, how some have come to imagine transparency obligations in European data protection law: an act of almost perfect communion between those who decide to process personal data (the ‘data controllers’) and the individuals linked to such data (the ‘data subjects’), during which the latter get to actually see, and properly understand, what is going on with their data, why this is occurring at all, what will happen to them and their data in the near future, and what they could do about it, in case they would like to do something about it. A short moment of illumination of the nevertheless generally unaware individuals that comprise a predominantly ignorant population. The great lifting of the veil of the ever so obscure global contemporary data practices. A ray of light amidst the darkness. The joy of unravelling the precise manner in which you are being profiled. The ecstasy of personal enlightenment, in which ‘being aware’ (van der Hof and Prins 2008, 119) and ‘opening up’ (Benoist 2008, 181) are the keywords. The last hope in an increasingly in-transparent world, full of uninformed people.

Breaking open windows

Transparency, as its name suggests, could indeed be about finally being able to see through the shadows of opaque data processing operations. It could, in principle, be about revealing to data subjects the exact nature of what is really going on whenever somebody collects data about them, by bringing those ignorant individuals in direct contact, face to face, with what is happening, and what is - potentially - going to happen at some point. To finally make palpable to everybody the

authentic fabric of data processing. To allow you to put your fingers into the spaces between the muscles of the algorithms shaping your existence.

In European data protection law, however, transparency is fundamentally not about a vague, utopic state of objective clarity, but about something else. It is not about letting data subjects sneak into the real life of their data and into the algorithms that move them, but about providing individuals with a certain narrative about all this processing; a narrative de facto constructed for data subjects on the basis of the interests of the data controllers, and adapted to fit a certain idea of the data subject's presumed needs and ability to discern. At its core, transparency is indeed not about disclosing any hidden practice, or about bringing data subjects closer to anything at all, but about generating and adapting a certain data story to an imagined data reader, that is, about re-creating and triggering new accounts about data, built on some data visions.

Transparency is, in this sense, about translating, and creatively transcribing and delivering to data subjects an account of what is being done to their personal data, tailored to a certain idea of what individuals might want to hear, and what they can perceive. It is about being told how you are being profiled, but in a language that inevitably betrays you were already 'being profiled' in order for controllers to decide how they would tell you about it.

The GDPR says it clearly and concisely

Concretely, transparency in European data protection law is an obligation imposed on data controllers to communicate a series of pieces of information, and to communicate them 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language' (Art. 12(1) of the General Data Protection Regulation (GDPR)).¹ Beyond the tautological assertion according to which transparency is about communicating something in a "transparent" way, what the quoted GDPR provision expresses is that transparency is about making an effort to convey information in a way that is objectively short ('concise') and simple ('using clear and plain language'), but also in a manner that is subjectively and contextually adapted to the ability of the addressed data subjects to grasp its meaning, and to make some sense of it. Transparency is, in this way, about a certain reading of who is expected to read transparency notices, and a writing of such reading into the text data subjects will finally get to read.

Complying with the obligation of transparency imposes indeed on the data controller the prior obligation to determine – deliberately or not, consciously or not – who are the targeted data subjects, and what are they supposed to find intelligible and easily accessible. This therefore demands from controllers, first, to take a stand on who might be these individuals (to somehow imagine them, and speculate on their comprehension skills), and, second, to attempt to communicate in a way that presumably matches the intelligibility requirements derived from such imagined/imaginary data subjects.

In this sense, the information provided by controllers to data subjects reflects the controller's perception of the individuals whose data they are about to process; the communication of this information is shaped by such reflection, and sustains it. It is more than just pure plain language, clinically and concisely arranged in an objectively clear manner. It is not an open door towards their own data practices, or an open window into accompanying data protection safeguards. It is not a veil that is lifted, but a veil that is woven. It is a translation to the extent it is framed by the author through an invented data subject/reader, and participates in the further invention of such a subject/reader – it is a 'gesture of appropriation' (McDonald 1988, 152), and an act 'mediated and filtered through the opacity of writing' (Murail 2013).

Tell me you can read me

This translation, technically speaking, shall precede the (second) translation that comes in when the personal data processing at stake actually begins. That is the moment when the data controller can

formally start building its own data construction of the individuals whose data it processes, on the basis of the data collected from them, and/or from other sources.

In practice, there is nevertheless often a temporal grey zone surrounding the moment when the data controller starts processing data, on the one hand, and the moment when 'transparent' information is given to the data subject, on the other. Although information shall, in principle, be provided 'at the time when personal data are obtained' from the data subject, it appears that some data controllers do feel entitled (and possibly obliged) to process beforehand at least some data, such as data that will help them determine in which language the data subject needs or deserves, in their view, to be told about the just-about-to-begin data processing practices and correlated data protection safeguards.

Living nearby or inside a linguistic border, and within a linguistically complex reality, it is for instance particularly easy to witness variance in automated language selection decisions, typically unilaterally taken by controllers on often persistently unclear grounds. In my personal case, for instance, the social networking site Facebook has decided I must read their 'Facebook Data Policy' in French, and thus I might repeatedly click and re-click on a link called 'Facebook Data Policy', but I will systematically be automatically directed to a page titled '*Politique d'utilisation des données*', in French.² The digital music service Spotify, on the contrary, initially judged I shall rather read their Privacy Policy in Dutch, and directed me insistently to it for some time, although now it does allow me to cheat and pretend I live in the United Kingdom to access it in English, and thus be able to quote here the beautiful passage where it is stated that my privacy 'is, and will always be, enormously important' to them, and that therefore they 'want to transparently explain how and why [they] gather, store, share and use [my] personal data'.³

These are mere examples of choices made by data controllers to define how data subjects can learn about ongoing and upcoming processing operations that affect them and the data connected to them, illustrating that transparency is, foundationally, mediation.

A pixelated mirror in front of a pixelated mirror

Once we agree that to 'transparently explain' is to sustain a certain (pre-)conception of what data subjects need to – and can – understand, this necessarily obliges us to move beyond any simplistic debates about whether what is needed is 'more' or 'less' transparency, or about whether transparency is either 'good' or 'bad'. Transparency is not to be measured by degrees, nor to be celebrated or dismissed as such. It is not about showing, or giving access, but about interpreting and creatively rendering and supporting a certain image of targeted individuals. Transparency is not something that happens to counter the fact that individuals are being profiled, but already about 'being profiled'. Once we realize that transparency is translation, we can move out of naive metrics and binary politics of transparency, towards a critique of how it qualitatively modulates power relations between data controllers and (data) subjects.

Notes

* Gloria González Fuster is a Research Professor at the Vrije Universiteit Brussel (VUB)'s Faculty of Law and Criminology. Member of the Law, Science, Technology and Society (LSTS) Research Group and of the Brussels Privacy Hub (BPH).

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).

² Politique d'utilisation des données, Date de la dernière révision: 19 avril 2018, https://www.facebook.com/policy.php?CAT_VISITOR_SESSION=c7b73ebc78d1681ade25473632ea e199 [last accessed 10th June 2018].

³ Spotify Privacy Policy, Effective as of 25 May 2018, <https://www.spotify.com/uk/legal/privacy-policy/?version=1.0.0-GB> [last accessed 10th June 2018].

References

- Benoist, Emmanuel. 2008. "Collecting Data for the Profiling of Web Users." In *Profiling the European Citizen*, edited by Mireille Hildebrandt and Serge Gutwirth, 169–84. Dordrecht: Springer.
- Hof, Simone van der, and Corien Prins. 2008. "Personalisation and Its Influence on Identities, Behaviour and Social Values." In *Profiling the European Citizen*, edited by Mireille Hildebrandt and Serge Gutwirth, 111–27. Dordrecht: Springer.
- McDonald, Christie V., and Jacques Derrida. 1988. *The Ear of the Other: Otobiography, Transference, Translation; Texts and Discussions with Jacques Derrida*. Lincoln: University of Nebraska.
- Murail, Estelle. 2013. "The Flâneur's Scopic Power or the Victorian Dream of Transparency." *Cahiers Victoriens et Édouardiens (Online)* 77 (Spring). <https://journals.openedition.org/cve/252>.