Data Protection without Data: Could Data Protection Law Apply without Personal Data Being Processed?

Dara Hallinan*

Broadly put, European data protection law is concerned with providing individuals with protection against harms connected with the collection and processing of their information. One set of harms data protection is concerned with relate to disproportionate behavioural change and self-censorship resulting from information processing activities: chilling effects connected with information processing. The idea that this form of harm is a matter of consequence for data protection law has jurisprudential support. This support was vocalised in the Court of Justice of the European Union (CJEU) Digital Rights Ireland case. In this case – on data retention – the Court expressed concern that:

the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.\(^1\)

Chilling effects connected with information processing can arise when information about an individual is processed and the individual, aware of an act of surveillance, amends their natural behaviour to fit with some presumed normative standard. Yet, the actual collection and processing of information is irrelevant to the causation of these chilling effects. The only relevant causative factor is that the individual believes information about them is being processed. Accordingly, chilling effects connected with information processing can also arise when the individual merely believes information about them has been collected and processed although this is not, in fact, the case. For the purposes of this contribution, such chilling effects

---

DOI: 10.21552/edpl/2019/3/5

* Dr Dara Hallinan, FlZ Karlsruhe, Germany. For correspondence: <Dara.Hallinan@flz-Karlsruhe.de>. I would like to thank Bart van der Sloot and Diana Dimitrova for their insightful and useful comments on previous versions of this contribution.

\(^1\) Case C-293/12 Digital Rights Ireland Ltd [2013] ECLI:EU:C:2013:845, Opinion of Advocate General Cruz Villalón, paras 52 and 72.
involving no processing of information will be referred to as ‘informationless chilling effects’.

The identification of the possibility of informationless chilling effects may seem rather academic – theoretical, with little correspondence to reality. There are, however, concrete instances in which informationless chilling effects are highly relevant. One example is the deployment of dummy camera systems. Dummy camera systems work on the basis that the individuals perceiving the dummies will presume information about them is being collected and processed – that the cameras are filming and recording – and will alter their behaviour accordingly. Dummy cameras and informationless chilling effects have already been thematised in certain European states’ law. In Germany, for example, the District Court of Frankfurt/Main obliged the removal of a dummy camera system, highlighting informationless chilling effects as a harm to the plaintiff’s general personality rights. In Norway, the 2018 Personal Data Act – in Article 31 – includes specific provisions dealing with dummy cameras on the same grounds.

On the basis of the above, the following argument might be made: if informationless chilling effects are a sub-category of chilling effects concerning information processing, and chilling effects concerning information processing constitute harms forming the subject matter dealt with by European data protection law, then informationless chilling effects should also constitute the subject matter dealt with by European data protection law. This line of argumentation leads, logically, to the following question:

Should concrete legal manifestations of European data protection law – particularly the General Data Protection Regulation (GDPR) – apply to systems and activities which engage informationless chilling effects?

Whilst the supporting argumentation is straightforward, the idea that concrete manifestations of European data protection law should apply to systems and activities

---

2 That chilling effects can manifest without information processing should be no surprise. The constitutional concept of a chilling effects refers to activities which place doubt or fear into an individual’s mind such that they refrain from engaging in legitimate behaviour. The European Court of Human Rights (ECtHR) relies frequently on the doctrine in relation to the effects of punitive sanctions on free speech. The Court stated in the case of Altuğ Taner Akçam, for example: ‘The Court...notes the chilling effect that the fear of sanction has on the exercise of freedom of expression, even in the event of an eventual acquittal, considering the likelihood of such fear discouraging one from making similar statements in the future’. Altuğ Taner Akçam v Turkey App no 27520/07 (ECtHR, 20 January 2012), para 68.

3 The Court stated: ‘The threat, associated with the installation of a dummy camera, of the surveillance of the movements of the plaintiff and his visitors in the entry to the house, constitutes a restriction of his general freedom of action which would only be legitimate under specific circumstances’. Author translation of: ‘Bereits die mit der Anbringung einer Attrappe verbundene Androhung der ständigen Überwachung der Bewegung des Klägers und seiner Besucher im Haupteingangsbereich stellt eine Beeinträchtigung seiner allgemeinen Handlungsfreiheit dar, die nur unter besonderen Umständen zu rechtfertigen ist.’ AG Frankfurt/Main Az: 33 C 3407/14 [2015] 2.


engaging informationless chilling effects immediately calls forth several objections. Four seem particularly powerful:

1. Informationless chilling effects do not arise from the processing of information about individuals and are not informational harms. Informationless chilling effects, therefore, do not constitute the type of harms dealt with by European data protection law.

2. European data protection law has historically focused on systems and activities involving information. To apply data protection law to systems and activities excluding information would be problematic for the conceptual integrity of the area of law.

3. As a key scoping concept, European data protection law has traditionally required that ‘personal data’ be processed. One of the key defining criteria for the presence of ‘personal data’ is that ‘information’ is processed. In systems engaging informationless chilling effects, no ‘information’ is processed and therefore data protection law cannot apply.  

4. The substantive principles of European data protection law have been designed to directly regulate information flows. The application of these substantive principles to systems or activities involving no information will be logically difficult, if not impossible.

As powerful as these objections initially seem, however, the argumentative walls they erect are not impenetrable.

In response to the first objection: the objection is superficially understandable – systems and activities engaging informationless chilling effects do not involve the collection or processing of information. A deeper look, however, shows the objection to be disingenuous. Informationless chilling effects are inextricably connected with information processing activities. Systems and activities engaging informationless chilling effects can only manifest in specific contexts. These contexts are defined by the pervasive presence of superficially equivalent systems or activities – visually or procedurally – which do involve the collection and processing of information about individuals. Only in these contexts can the mimicking of the symbolism of these systems or activities – emblematic of systems engaging informationless chilling effects – produce pavlovian behavioural responses on the part of individuals. Informationless chilling

---

6 A version of this argument seems to have been put forward by the European Data Protection Board in their conclusion that the GDPR cannot apply to dummy cameras: ‘The GDPR is not applicable for fake cameras (i.e. any camera that is not functioning as a camera and thereby is not processing any personal data).’ Close reading of the document outlining the position, however, reveals the position could relate to the unidentifiability of data subjects by dummy cameras. If this latter reading of the EDPB opinion is correct, then an obvious retort is that there are many other ways in which an individual could be identified as the subject of a system engaging informationless chilling effects – for example, registers recording individuals’ presence in a system or activity space, self-presentation by an individual as a subject to a data controller. European Data Protection Board, ‘Guidelines 3/2019 on processing of personal data through video devices (Version for public consultations)’ (EDPB Plenary meeting, 9-10 July 2019) 5. Thanks to Raphael Gellert for bringing this to my attention.
effects are thus completely parasitic on information processing activities. Informationless chilling effects, therefore, cannot be described other than in terms of informational harms.\(^7\)

In response to the second objection: it is true that applying data protection law to systems or activities engaging informationless chilling effects would represent a conceptual break with the status quo. The fact that a novel application of data protection law would constitute a break with the status quo, however, is not problematic. In its short 50-year history, data protection law has gone through multiple significant evolutions – in terms of the problems law sought to solve and the substantive approaches law took.\(^8\) Indeed, the need for data protection law to evolve to address phenomenological and social change is even hardwired into the GDPR. Consider, for example, the broad powers given to data protection authorities and to the European Data Protection Board to adapt and amend the GDPR to deal with novel developments in data processing.\(^9\) If change itself is par for the course, the only remaining question is whether an extension of applicability would constitute legitimate change.

In relation to this question, the legitimacy of conceptual change in the applicability of an area of law will be context dependent. Several contextual factors deserve consideration, amongst which the following seem particularly relevant: the aims the law seeks to achieve, user expectations as to the subject matter and flexibility of the law, and the position of the law in a broader ecosystem of laws. In relation to each of these factors, arguments for the legitimacy of extending the applicability of European data protection law to systems and activities engaging informationless chilling effects can be made. Arguments as to the teleological legitimacy of an extension have already been sketched above. Arguments that the extension would fall within users’ expectations can be made on the back of the teleological argument supported by the constant change of data protection law to date.\(^10\) Finally, arguments as to the legitimacy of the extension, considering data protection law in an ecosystem of laws, can be

---

\(^7\) How informationless chilling effects should be categorised in a taxonomy of informational harms is an interesting question. Laurie engages with a comparable case. The case involves the return of genetic test results to unsuspecting individuals capable of causing psychological harm to those individuals – for example the psychological harm caused to individuals who learn they are predisposed to Huntington’s disease. Laurie proposes that such harms might be regarded as a type of harm to privacy rights, as an unwarranted invasion of a private psychological sphere. Graeme Laurie, Genetic Privacy: A Challenge to Medico-Legal Norms (Cambridge University Press 2002) 64. Other categorisations are, however, equally imaginable. One might argue, for example, that harms emerging on the back of feelings of being watched fit better with concepts of mental integrity rights or freedom of thought rights. Each categorisation will have strengths and weaknesses.

\(^8\) Consider, for example, the first data protection laws and their focus on addressing the societal risks – for example those associated with the establishment of inhuman bureaucracies and the disturbance to the balance of executive and legislative power – arising from state mainframe-based processing. Compare these laws with the GDPR and its focus on harms to individual rights in relation to both state and private processing. See, for an overview of the development and evolution of European data protection law: Viktor Mayer-Schönberger, ‘Generational Development of Data Protection in Europe’ in Phillip Agre and Marc Rotenberg (eds), Technology and Privacy: The New Landscape (MIT Press 1997); Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU (Springer 2014); Orla Lymsky, The Foundations of EU Data Protection Law (Oxford University Press 2015).

\(^9\) The GDPR grants the Board, under art 70(1)(e), the power to ‘[exam[ine]…any question covering the application of this Regulation’. As De Hert et al observe, the GDPR foresees a: ‘strong and standalone Board…capable of deciding…and enforcing…opinions [when interpreting the Regulation]’. Paul De Hert and Vagelis Papakonstantinou, ‘The new General Data Protection Regulation: Still a sound system for the protection of individuals?’ [2016] 32 Computer Law and Security Review 179, 194.

\(^10\) That certain national data protection laws already include provisions dealing with instances engaging informationless chilling effects – see, for example, the Norwegian Personal Data Act 2018 discussed earlier in this piece – speaks for the possibility that an extension will fall within expectations.
made via reference to the fact that no other area of law obviously deals with the issue.\footnote{11}{See, for a discussion of the potentially huge scope of data protection law and the place of data protection in an ecosystem of laws dealing with informational harms: Nadezhda Partova, ‘The law of everything. Broad concept of personal data and future of EU data protection law’ [2018] 10(1) Law, Innovation and Technology, 41.}

In response to the third objection: interpretations of the concept of information in data protection law encompassing systems and activities engaging informationless chilling effects can be offered. The legislative history and jurisprudence around the concept of information in European data protection law reveals a concept with boundaries defined teleologically – in relation to the overarching goals of the law.\footnote{12}{See, for example, the elaboration of the Article 29 Working Party of the concept of information in their opinion on the concept of personal data: ‘The term “any information” contained in the Directive clearly signals the willingness of the legislator to design a broad concept of personal data. This wording calls for a wide interpretation.’ Article 29 Data Protection Working Party, ‘Opinion 4/2007 on the concept of personal data’ (2007) WP136, 6. The Working Party outline a circular logic – ‘any information’ means the need for a broad concept of personal data. This circular logic makes sense only when the concept is read in light of the overarching aims of the GDPR, as outlined in art 1(2): “[the protection of] fundamental rights and freedoms [engaged by the processing of information about individuals].”}

Thus, the boundaries of the concept of information in data protection eventually stretch to encompass whatever substance engages the types of harms dealt with by data protection. It is true such a concept of information is not resonant with concepts of information used in other disciplines – for example in computer science.\footnote{13}{See, for a discussion of this lack of resonance: Dara Hallinan and Paul De Hert, ‘Many Have It Wrong – Samples Do Contain Personal Data: The Data Protection Regulation as a Superior Framework to Protect Donor Interests in Biobanking and Genomic Research’ in Brent Mittelstadt and Luciano Floridi (eds), The Ethics of Biomedical Big Data (Springer 2016) 119, 130-139. See also: Dara Hallinan and Raphael Gellert, ‘Two Concepts of Information in Data Protection Law’ (2019 Forthcoming).}

There is, however, no indication a concept of information from another discipline was intended as a template for data protection law.\footnote{14}{There is no indication of the desire to use a definition from another discipline as a template in any policy document relating to either Directive 95/46 or the GDPR. As Bygrave observes: ‘we often cannot be sure whether the architects of data protection law have applied such an understanding of data and information’. Lee Bygrave, ‘The Body as Data? Biobank regulation via the ‘Back Door’ of Data Protection Law’ [2010] 2(1) Law, Innovation and Technology 1, 14. Indeed, given that the boundaries of concepts of information in other disciplines also tend to be drawn teleologically – for example, according to scientific utility, as in biology – a transplant of a concept of information taken from any other discipline into data protection law would likely be highly awkward.}

Nor is there any reason to think data protection law should not employ a *sui generis* concept of information. After all, data protection employs other *sui generis* definitions of concepts found in other disciplines – there is only partial overlap, for example, between the concept of ‘genetic data’ in the GDPR and the concept of genetic data used in biology.\footnote{15}{The definition in art 4(13) states: ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question’. This definition would exclude several aspects of the concept of genetic data as used in biology. The definition would, for example, exclude the conceptualisation of the DNA in the biological sample itself as genetic data as well as information on an individual’s genome extracted via methods other than analysis of DNA – for example visually, by reference to a physical phenotype rooted in specific genetic architecture. See, for a discussion of the limitations of the concept of genetic data in the GDPR: Dara Hallinan, ‘Feeding Biobanks with Genetic Data: What role can the General Data Protection Regulation play in the protection of genetic privacy in research biobanking in the European Union?’ (VUB Doctoral Thesis, 2018) 299, 305.}
non-sensical. There are, however, other provisions in the GDPR which, although initially designed to deal with information, could conceptually and practically be adapted to deal with systems engaging informationless chilling effects. Examples would be transparency provisions – such as those in Article 13 – and the necessity principle in Article 5(1)(c). There are yet other substantive provisions in the GDPR which do not employ information specific approaches at all. The meta-regulatory approaches offered by Articles 25 – data protection by design – and 35 – data protection impact assessment – are particularly interesting in this respect.

These meta-regulatory principles oblige data controllers to conduct an assessment of harms associated with prospective operations and to design and adopt suitable and adequate safeguards in relation to these harms. These principles apply regardless of the types of harms brought forward by a system or activity, the types of safeguards to be adopted in relation to these harms and as to whether relevant safeguards are explicitly mentioned elsewhere in the GDPR. Such meta-regulatory provisions could logically be applied to provide protection in relation to systems and activities engaging informationless chilling effects. Adherence to these provisions is subject to the same oversight and sanctions regime as is applicable to other substantive provisions. It might be argued that the selective applicability of data protection principles would be a violation of the logic of data protection law. The possibility of selective application of principles, however, has jurisprudential support. As the Article 29 Working Party observed: ‘where processing of personal data within the scope of the [law] is involved, not all the rules…may be applicable in the particular case’.

The above argument sketches the rationale for the applicability of European data protection law to systems and activities engaging informationless chilling effects. The argument does not, however, mandate urgent legal action. There is currently limited use of systems and activities engaging these harms. Consequently, the harms are of limited social significance and are the subject of little legal or academic investigation. Given the absence of incidence and investigation and given data protection was not

---

16 In terms of transparency provisions: a controller could provide all affected individuals with a great deal of data about the system or activity in question without even touching on the fact that information were not being processed – for example, the identity of the controller and the purpose of the system or activity. Provisions could also be interpreted in a context dependent manner such that, where it would make sense, certain individuals would need to be given more more information about the true functioning of the system – including that information are not being processed. In terms of the necessity principle: the principle could be read to encompass considerations of whether the deployment of the system or activity was necessary in relation to the ends sought alter at all – in traditional proportionality calculation fashion.


18 Article 29 Data Protection Working Party, ‘Opinion 4/2007’ [n 12] 5. Indeed, from a long-term perspective, the idea of one set of data protection principles applicable across all contexts seems untenable. Data protection relates to a vast array of types of actors, activities, technologies, information and affected individual. Each constellation of these factors breeds specific risks of harms requiring, ideally, unique legal responses. For example, it becomes increasingly clear that factual and inferential personal data have significantly different qualities and are not easily subject to the same set of data protection principles. See, for example: Sandra Wachter and Brent Mittelstad, ‘A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI’ [2019] 2 Columbia Business Law Review, 494. As the regulatory needs of each factor, and constellations of factors, crystallise over time, data protection will likely sub-divide into factor, and constellation, specific rules. The need to specify data protection principles to deal with specific situations has already been recognised in the GDPR. For example, the need for further specification of data protection principles for specific processing contexts was foreseen in the legislative process. See: European Commission, ‘Impact Assessment Accompanying the General Data Protection Regulation’ (2012) SEC(2012)/72 final, 65-74. Equally, certain substantive principles – for example art 21 on automated individual decision making – already apply to specific information processing technologies and deployment contexts.
designed for informationless chilling effects, an extension would, currently, be premature. Nevertheless, the exigency of the argument will grow. Information society processes will increasingly become background social presumptions and will increasingly engender predictable behavioural responses: fertile ground for systems and activities engaging informationless chilling effects. Legal responses will become necessary. Intuitively, *sui generis* legal approaches would seem the most logical approach. In the case these are not expediently forthcoming – and we should not hold our breath that they will be – data protection law is the next logical venue to look for solutions.