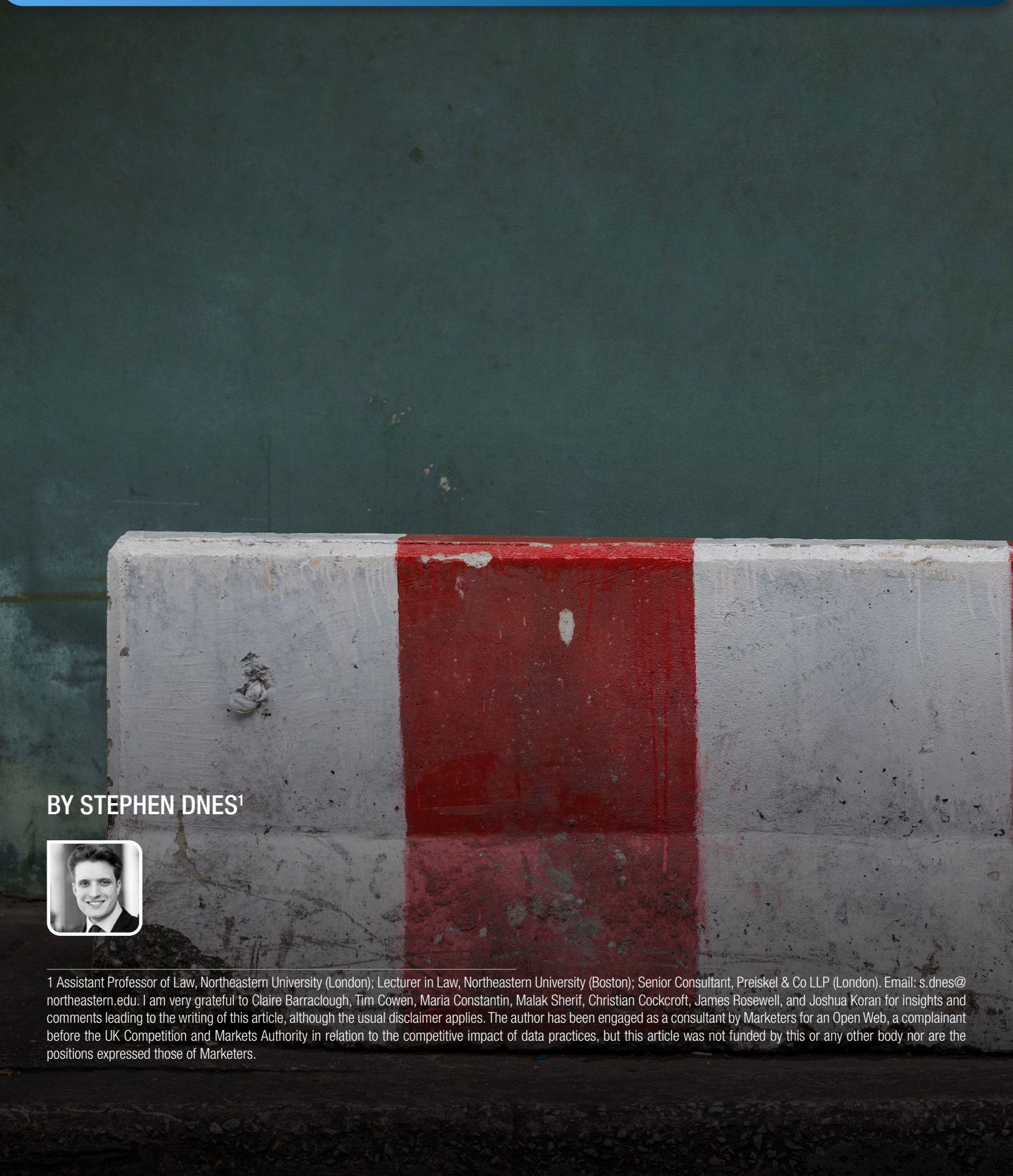
BIG DATA PROTECTION: BIG PROBLEM?



BY STEPHEN DNES[1]

1 Assistant Professor of Law, Northeastern University (London); Lecturer in Law, Northeastern University (Boston); Senior Consultant, Preiskel & Co LLP (London). Email: s.dnes@northeastern.edu. I am very grateful to Claire Barraclough, Tim Cowen, Maria Constantin, Malak Sherif, Christian Cockcroft, James Rosewell, and Joshua Koran for insights and comments leading to the writing of this article, although the usual disclaimer applies. The author has been engaged as a consultant by Marketers for an Open Web, a complainant before the UK Competition and Markets Authority in relation to the competitive impact of data practices, but this article was not funded by this or any other body nor are the positions expressed those of Marketers.

Interoperability: The Wrong Prescription for Platform Competition
By Jay Ezrielev & Genaro Marquez

Self-Preferencing and Antitrust: Harmful Solutions for an Improbable Problem
By D. Bruce Hoffman & Garrett D. Shinn

The Unilateral Conduct Gap Sacrificing Interoperability and Innovation
By Susannah P. Torpey & Dillon Kellerman

Interoperability in Antitrust Law & Competition Policy
By Laura Alexander & Randy Stutz

Big Data Protection: Big Problem?
By Stephen Dnes

How Self-Preferencing Can Violate Section 2 of the Sherman Act
By Daniel A. Hanley

Interoperability as a Lens onto Regulatory Paradigms
By Chris Riley & James Vasile

Invigorating Competition in Social Networking: An Interoperability Remedy That Addresses Data Network Effects and Privacy Concerns
By Cristian Santesteban & Shayne Longpre

Data Protection Overkill: The World's Biggest Barrier to Interoperability?

By Stephen Dnes

Considerable debate exists as to the interaction of antitrust and privacy law. This nuanced debate encompasses many difficult questions: when is there a strong consumer preference for privacy, and when is there not? Under what circumstances do consumers happily trade data for service access? In an online world characterized by large platforms, is data collection a feature or a bug, and are the terms competitive? Can consumers and publishers internalize possible externalities from data use, or are there incentives for data processors to generate external costs? All these questions have profound implications for interoperability, because they affect how much use can be made of data across systems: the stronger the data protection right, the weaker the prospects of interoperability. The purpose of this article is to note significant moves in recent months towards a more consumer-centric approach to answering these questions. There is a prospect of using a well-known competition law device – the consumer welfare standard – to unite competition and privacy analyses, placing the consumer interest at the heart of the answers to these crucial questions.

I. PERSONAL QUESTION: ROCKY ROAD OR COOKIE DOUGH?

It is a hot, sunny day. A gentle breeze is blowing in from the sea. You have just spent a wonderful afternoon at the beach gazing out at the horizon with an excellent beach read — and no, it is not an antitrust journal. You left your phone in the car — deliberately. What could top this bliss? Well, how about a delicious ice cream?

There is a line at the entrance to the ice cream parlor. You eye up the flavors chosen by the patrons in front of you as you wait — anxious to gain an early insight into the treasures in the cooler. When your turn comes, you make your choice and head happily back to the beach. Fellow beach goers see your ice cream, and it appears that you have set a trend, as they head to the parlor as well.

So far, you could be forgiven for thinking that the example is trivial. Who could possibly mind whether people know a readily accessible, humdrum piece of information like your choice of ice cream flavor? Yet when you saw the choices made by others in the ice cream parlor, did you not gain some data about your fellow beach goers? And when you were seen by others on the beach, did they not gain some data about you? Especially if you stopped at the car to pick up a beach umbrella: that license plate number is an identifier and, if recorded in a computer system, surely means we are firmly in the world of personal data! After all, the link between your car choice and your ice cream may be public, but it was not "manifestly" made public *by you* as required so as to be classed as exempt public data under the strict terms of Article 9 GDPR. You cannot eat an ice cream at the parlor other than in public, so how was it *you* who "manifestly" created the publicity? And more importantly, there is a law requiring license plates, so it can hardly be said that the plates were made public *by you*. Someone should pass a law to stop people knowing that drivers of cherry red convertibles like rocky road ice cream!

It is a common observation that data is just like the "grains of sand on a beach": ubiquitous, and even if not always easily accessed, certainly something which is always around us, at least in its unprocessed form. Indeed, sand can be made into many useful things: glass, concrete, cement, golf course sand traps. This is where things get difficult for interoperability. Suppose the ice cream parlor uses data to invest in the most popular flavors, and perhaps gives you a discount on your next visit. Imagine it has a loyalty app to help with this. Would it not have a major compliance burden, at least in the European Union, under the GDPR? Unless burdensome consent steps are taken under Art 6(1)(a) GDPR, which would be actively anti-consumer in a busy ice cream parlor, it is arguable that the requirements are not met: and the more processing and the more useful the data, the more must be asked under Art 6(1)(a) to achieve consent. There is no threshold at which the processor can say, *no one cares*; let alone, *it is net beneficial to the consumer not to ask*. So, there is personal data in the app; even if it is trivial, and useful in all conceivable applications, it is personal data nonetheless. Difficult and expensive pseudonymization rules apply, and even then, the GDPR only gives the benefit of a recital rather than a pass.[2] Nowhere is the question asked, is protection merited in the first place?

However pro-consumer the data use, still the regulatory burdens apply.[3] In a word: why? Despite no clear evidence of even the slightest risk of any consumer harm from innocuous use, the ice cream parlor is treated like Cambridge Analytica.[4] This creates a major barrier to interoperability in data: useful, albeit perhaps somewhat personal data, cannot be exchanged without detailed consent that may far exceed what consumers want; and useful data may be foregone as processing strictures like sample sizes are applied: red convertible + rocky road + Treasure Island + June 8th = 1 user, thus potentially identifiable data excluded by dint of GDPR. It is not an answer to point out that the consumer would

2 Article 25 GDPR encourages pseudonymization as a "privacy by design" measure, but it does not affirmatively allow this expensive step to be omitted where there is no consumer interest in privacy; nor does it create a safe harbor where pseudonymization is employed. Instead, recital 26 of the GDPR states: "data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person." This provision is stylistically verbose ("should be considered to be" = is), but more importantly, strips pseudonymization of safe harbor status since the risk of re-attribution is still a gate to liability, even if re-attribution poses no material consumer risk (e.g. attribution of ice cream flavor). It is also poorly drafted: if re-attribut*able*, why pseudonymous in the first place? It would be more helpful to define the concept better than to create a half-baked exception. It is notable that the California CCPA is somewhat more precise, though still far from a safe harbor: § 1798.140(r) - Pseudonymization "[M]eans the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer."

3 Article 25 GDPR refers to the context of processing, including cost, but still affirmatively requires "state of the art" protection, despite the possibility that this is not merited. It would be a brave business who would argue that "state of the art" can be interpreted to be zero, even where this is the pro-consumer outcome.

4 I am grateful to Sherif Malak for this colorful example.

want the parlor to know to have the ice cream ready, and would rather not be asked about this.[5]

Now imagine that the ice cream parlor has the temerity to sell the data on ice cream to a large concern interested in providing people with the products that they want. Or to a marketing consultancy, keen to identify trends in ice cream consumption — "Dairy Free ice cream: Fun free, or the future?" Perhaps a start-up beach app has nifty AI to combine data on length of beach stay, parking costs, the quality and number of sunset pictures, and the number of ice cream flavors available — a dynamic pro-consumer innovation, especially for time-poor holidaymakers or those unfamiliar with a stretch of coastline. Moreover, in a competitive market, the consumer benefits from the data sale even on a static analysis, as the sale will be at least partially passed on in lower prices.

Yet all of these are regulated uses, especially as data sources are combined, such that the GDPR's legalistic view of informed consent bites — and many of the uses cannot be specified by the ice cream parlor in advance since the end use, despite being pro-consumer, is unknown. Indeed, Article 25 GDPR specifically limits the ice cream parlor to the minimum processing necessary for *its* purposes.[6] This ignores relative competence and gains from specialization. The transfer follows from relative competence: sale of data *because* the parlor does not have the expertise in processing. The sale is economically efficient and pro-consumer — and for precisely this reason, informed consent cannot be obtained exactly where interoperability in data sets is most valuable. In effect, the GDPR forces the supervision of data collection to be vertically integrated, banning interoperability and harming competition.

If consulted on *why* this scale of protection is necessary, even for innocuous data, the legalistic GDPR instead repeats like a scratched vinyl record… "consent by the user… consent by the user… manifestly made public *by the user*…" The beachgoer would promptly tune out of that radio station — and with good cause. Instead of an assessment of relative risk of damage and consumer benefit, as would be routine in antitrust, there is instead a major compliance burden on combining the data: even though the large database, or analyst's report, or start up app, would simply be about ice cream trends and a nice day out at the beach.

II. CONSUMER WELFARE AS THE GATEWAY TO INTEROPERABILITY

A survey of the major GDPR definitions and requirements recalls the *Hound of the Baskervilles*: They are remarkable for what they do not do. Nowhere in the definitions is there direct analysis of consumer welfare. This in turn undermines interoperability in data. Yes, some *collected* data can sometimes be combined and traded, but there is a large "known unknown": potentially interoperable data which is never collected, because innocuous consumer data must still comply with potentially expensive requirements, even where this is actively anti-consumer by increasing costs and decreasing innovation.

This will be clearest from a redline edit on some of the most offending provisions. The underlines are edits on the GDPR from a pro-consumer point of view. Behold, the CDPR (*Consumer* Data Protection Regulation):

> **Data subjects: Art 4(1)**
> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person who has a reasonable basis for material concern about that data;
>
> **Data processing: Art 4(2)**
> 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction which, on the basis of reasonable evidence, is likely to give rise to consumer harm;

5 Very oddly, if the enterprise gets the data wrong (e.g. green convertible listed, not red), EU guidance suggests that GDPR does not apply at all as the information is then not personal under Art 4 GDPR: https://gdpr.eu/eu-gdpr-personal-data/. This is the height of legal formalism. The test appears to operate in opposition to the gathering of relevant data — the question unposed, much less answered, is: *Why should regulation change because of clerical error, as opposed to consumer-relevant risks and benefits from the decision to collect the data?*

6 Art 25(2) GDPR: "Only personal data which are necessary for each specific purpose of the processing are processed."

At a stroke, these two small edits would release innocuous use from any burden. Instead, the regulation would target only those practices harming consumers on an evidenced basis.

Profiling: Art 4(4)

'profiling' means ~~any form of~~ automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, ~~in particular~~ only to analyze or predict ~~aspects concerning that natural person's~~ identified categories raising evidenced concerns about performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements where these give rise to a material risk of consumer harm;

The CDPR drafter might note that "in particular" in Art 4(4) is vague, since almost any characteristic qualifies for the list that follows. If there is a concern, it should be specified on an evidenced basis: automation alone cannot be the concern, since that logic would object to *any* automation — a luddite superstition, unless there is evidence that the automation is causing a problem. A consumer might ask: why is a power to regulate in the absence of evidence of a problem needed, since principled regulation would always be able to show evidence of harm?

Consent: Art 6 1 (a)

Processing shall be unlawful only if ~~and to the extent that at least one of the following applies:~~ the data subject has not given consent to the processing of his or her personal data, ~~for one or more specific purposes~~ and only if such processing raises material consumer concerns;

…

(f) processing is demonstrably unnecessary, leading to harm, giving particular weight to harm to minors. ~~for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.~~

The CDPR drafter notes another vague provision: "one or more specific purposes": is an open-ended list acceptable then ("or more"), or not? Perhaps the CDPR should simply require evidence of harm, rather than dissect processes of consent.

More philosophically, further vagueness creeps into another crucial definition: "rights and freedoms." This ignores an important Anglo-American contribution to jurisprudence: Hohfeldian analysis of rights, based on the same well-known error in *Quinn v. Leathem*.[7] As Hohfeld noted, rights and freedoms are not the same thing and should not be used interchangeably.[8] The drafter appears to have in mind a right, creating duties in others, precisely to *curtail* liberties. This masks an important trade-off: the right curtails liberties (here, in data processing), and is this wise? The liberty interest might be just as important, but in a (possibly deliberate) sleight of hand, it is opaquely bundled in a mélange of rights-as-liberty.

A more precisely specified approach would identify *both* the right and liberty interest, and try to define a balance between their opposition, rather than (assertively) skating over the difference — not least as this avoids empowering the regulator to define a balance which might be better defined in law. This can easily be done by specifying which rights give rise to *which* duties, and when, carving out of a general starting position of liberty. It is routine in many areas of the common law: consider the duty of care in tort as one such departure from general liberty — only applicable where a duty of care can be shown to arise based on evidence; out of respect for liberty, there is no duty of care to smile, however beneficial this might be to others! Significantly, the consumer welfare standard in antitrust does the same — and could be used here to define the correct balance between the data protection right and the liberty interest of data processors, as explored further below.

Article 6(1)(f) also breaches a basic tenet of liberal enlightenment thinking: it reverses the burden of proof as regards data use, even where innocuous. "Necessary" for "legitimate interests" according to whom? A regulator subject to capture risks? By what standard? *Why* is it not specified? Contract law developed, at least in common law jurisdictions, *not* to ask these questions, and instead to defer to parties: the

7 [1901] AC 495.

8 Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning and Other Legal Essays* (1913 and 1919, pub'd Yale UP 1964). As early as 1980, this was said to be "…now a standard part of legal thinking." Walker, *Oxford Companion to Law* p. 575 (OUP, 1980) — but not, it would seem, in drafting the GDPR in Brussels.

starting point is that the spontaneous order is valuable and should not be lightly altered.[9] Certainly, if there is evidence of consumer harm, the question is different, and consumer protection laws or unconscionability doctrines would apply. But as a general proposition: the mere fact of use is suggestive of value, such that the law should not require justification, absent evidence of harm supporting tailored exceptions. Moreover, the provision violates the basic principle that the creator of new property, e.g. processed data products, has the strongest claim to it; if there are human rights in data, it is unclear why they do not extend to this proprietary interest, as well.[10]

With its many limitations in expression and philosophy, it appears that 6(1)(f) requires a complete redraft before it can be used in the CDPR. Rather than a final sub-section exception — notably, addressed after various state interests are listed — there should be a clear and crisp provision mandating evidence of consumer harm *before* justification is required. A new provision cutting across the entire edifice would appear to be required — limiting the power of regulators absent evidence of harm, and certainly not empowering them to decide for society what is "legitimate," unless evidence of harm can be shown.

As for Article 25, "Privacy by design," a simple edit would be that "state of the art" is only necessary where merited by demonstrated consumer needs.

III. THE CONTRAST WITH CONSUMER PROTECTION LAW

Perhaps the most curious point about the paternalistic stance of the GDPR is how much farther reaching it is than analogous EU law on consumer protection. The GDPR again seems not to take account of well-known debates. Consider the contribution by Bradner and Ulmer, requiring consumer protection law to leave core terms in consumer bargains to the market, immunizing them from challenge.[11] This has been implemented by exempting the price and other core terms in consumer transactions from challenge.[12]

The core terms exception is carefully framed to apply only to those core terms where shopping around is likely, e.g. price; this will sometimes be true for data (e.g. loyalty cards — discount for data) but the prospects of shopping around may sometimes be limited. However, the Bradner and Ulmer contribution paved the way for a balanced approach to evidence specification in consumer protection law. In contrast with the GDPR, this has been meticulously crafted to capture some, but not all, claims to consumer protection, thereby striking a balance between the market, and paternalism:

> A commercial practice is a misleading omission if, in its factual context, [it omits or hides] … material information… and as a result it causes or is likely to cause the average consumer to take a transactional decision he would not have taken otherwise.[13]

The same materiality requirement and protection of only the *average* consumer preference are seen in several other EU-derived consumer protection laws.[14] The balance was meticulously chosen: not all interests are protected; a regulator must put forward evidence of *average* consumer harm and materiality, to avoid the risk of over-regulation and to mitigate the risk of capture by special interests.

---

9 Consider the following common law contract rules: No assessment of adequacy of contract value: *Chappell & Co Ltd v. Nestle Co Ltd* [1959] UKHL 1 ("A peppercorn does not cease to be good consideration if it is established that the promisee does not like pepper and throws away the corn"); no general doctrine of unequal bargaining power: *Universe Tankships Inc. of Monrovia v. International Transport Workers' Federation* [1982] 2 All ER 67; risks of all but most serious mistakes to be managed by parties, not courts: *Bell v Lever Bros Ltd* [1932] AC 161; near-impossibility required, not just changed circumstances, before courts will invalidate obligations: *J. Lauritzen A.S. v. Wijsmuller B.V, ("The Super Servant Two")* [1990] 1 Lloyd's Rep 1. These tests all deliberately exclude vague references to "legitimacy," out of respect to party autonomy and the presumptive efficiency of the spontaneous order.

10 John Locke, Second Treatise of Government, Chapter V, paragraph 3: "Nor was this appropriation of any parcel of land, by improving it, any prejudice to any other man, since there was still enough and as good left, and more than the yet unprovided could use… Nobody could think himself injured by the drinking of another man, though he took a good draught, who had a whole river of the same water left him to quench his thirst." Provided that data flows — a principled threatened by GDPR — there seems to be a strong parallel between Locke's river and an innocuous data flow (e.g. information on ice cream flavors).

11 The authors noted that: "the consumer would no longer need to shop around for the most favourable offer, but rather could pay any price in view of the possibility of subsequent control of its reasonableness"
E Brandner & P Ulmer, "The Community Directive on Unfair Terms in Consumer Contracts: Some Critical Remarks on the Proposal Submitted by the EC Commission" (1991) 28 Common Market Law Review 647, p 656.

12 See e.g. UK Consumer Rights Act 2015, s.64.

13 See e.g. Regulation 6, Unfair Terms in Consumer Contracts Regulations 2008, the UK implementation of Directive 2005/29/EC.

14 See e.g. UK Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013, Rules 10 and 13.

Significantly, this also helps force the use of necessarily scare enforcement resources into consumer-relevant issues, e.g. is the fuel mileage accurate? Are the power and emissions figures reliable? What are the warranty terms? Few consumers would have much if any interest in how the electronic systems in the car intercommunicate, or the strength of the structural steel used in the body, and the car connoisseur's esoteric preferences are left to general contract law and the market since they fail the test of average consumer materiality.

It is unclear why a materiality test would apply to consumer protection law in general, but not to data use. The underlying concepts are identical: arguable market failure from unequal information or bargaining power; possible economic efficiency from requirements to flush information out into the market, to allow preferences to be revealed. Yet when buying a car, a materiality test based only on the average consumer applies; but it does not when signing up to the car dealer's newsletter.

It can hardly be argued that the average consumer is more informed about a modern car than about a newsletter email address storage system, and the consumer would presumably desire more protection in the larger purchase (although it should be noted that this is not the same thing as showing the net merits of protection). The legal protection appears to be exactly the wrong way around, and is even anomalous within the terms of other EU regulation.

IV. THE NEED FOR A RISK-BASED APPROACH

None of this is to say that there are not evidence-based consumer harms from data abuse. Well-known examples include the 2017 Equifax data breach, which released sensitive digital identity data of as many as half of Americans — despite evidence of foresight of a problem.[15] The oddity in the GDPR, seen through a competition telescope, is that nothing appears to be done to prioritize these risky cases: even if regulators can exercise triage and look only at the worst cases — objectionable anyway from a common law rule of law perspective for its excessive discretion[16] — the compliance burden is broader. Why not frame the law so that the compliance efforts address issues like those in Equifax, and not the car dealer's newsletter? Is that not a marginal improvement in the application of scarce resources?

There may be difficulties in gathering evidence from consumers on consumer harm. There is a significant gap in data on *subjective* consumer preferences relating to data protection. In its influential report on online markets, the UK CMA specifically notes a gap in the literature:

> "Few surveys examine what UK consumers perceive the specific benefits or harms of data processing and targeted advertising to be. Instead, consumer surveys tend to focus on the high-level benefits and harms resulting from all forms of online targeting."[17]

There is some survey evidence that consumers would like more protection of their data. However, as the CMA notes, these studies are high-level, and often fail to identify trade-offs, e.g. free content vs data retention. This is not unlike asking whether someone would like more pay, a larger car, etc.: yes please, to the free lunch. In the rare studies asking about the trade-off, consumers offer answers which are inconsistent with their revealed preference, e.g. stating that they would pay to retain more data, yet not giving preference to sites behind paywalls. For instance, an influential 2016 study noted that only 15 percent of consumers saw an exploitation risk from data, yet 57 percent disagreed with the statement that they were willing to give access to personal information for free access to a website.[18] 69 percent thought that they did not benefit from the sale of data to other companies, yet presumably a large number had benefited from free newspaper access, cheaper phones, etc., under precisely such a business model: the examples given by the survey were nowhere near the level of specificity to identify a tradeoff, let alone require consumers to reveal a preference. Indeed, a recent charitably funded study went so far as to call this a "web of paradoxes."[19]

15 See U.S. Federal Trade Commission, Equifax Data Breach Settlement, available at https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

16 A.V. Dicey, *Introduction to the Study of the Law of the Constitution* (1885; Macmillan reprint, London 1915).

17 CMA (2020) Appendix L: para 285. *Summary of research on consumers' attitudes and behaviour.*

18 See e.g. IPSOS, "Digital Footprints: Consumer concerns about privacy and security" (Nov. 2016), p.45-52.

19 P. Akman, "A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets," April 28, 2021, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3835280.

It may be that consumers are ill-placed *subjectively* to identify harms under existing systems: but this would be an argument for assessing *other* evidence of consumer harm, rather than to assume harm. The point then is that *objective* evidence of market failure should be collected — not that harm should be assumed.

It will immediately strike the antitrust lawyer that this is exactly the same question asked under the consumer welfare standard: is the average consumer harmed? What is the evidence? Subjective evidence of consumer harm is not the point: the point is to enhance economic efficiency through well-functioning markets, driving growth. There is no obvious reason why data protection should not apply a similar concept, to ensure relevance from the consumer point of view, rather than from the point of view of producers or regulators.

V. FOREGONE INNOVATION: INTEROPERABILITY ISSUES AND REGULATORY CAPTURE

The greatest concern from the lack of focus on consumer outcomes in the GDPR shows up in limited interoperability of data sets: unless the GDPR requirements are met, the data is non-compliant and cannot be used, regardless of the balance of consumer harm and benefit from the activity. This creates a powerful barrier to entry in the collection of data by new entrants, and tilts the data market towards large, established providers who have existing data troves.

Indeed, as regulation increases, the more valuable these existing troves become. There appears to be no prospect of disgorging over a decade's collection of past data, even if arguably non-compliant: the regulator worries only about the new data, potentially creating market power in the existing data. Legacy concepts are still in use, like first-party and third-party data, which *deliberately* aim to undermine interoperability: click once on a mega-platform, and you may have consented to significant data processing; but Bob's AdTech needs a new consent click and cannot sell or combine its data until it goes back to get consumer permission to innovate — a powerful tilt towards vertically integrated models, and a de facto ban on later innovative use that was not foreseen.[20] This fails the first rule of innovation, as noted by the Nobel prize winning economist Phelps. It is worth quoting his comment on this in full:

> "Innovations… are not determinate from current knowledge, thus are not foreseeable. Being new, they could not have been known before."[21]

In other words. the GDPR, in its informed consent requirement, applies the fallacy that innovations can be foreseen. This gives little to no weight to innovative use from interoperating data sets.

By contrast, the antitrust experience is that competition in vertically related markets has sometimes been an important spur to innovation — consider the well-known examples of the PC hardware and software markets, or long-distance telephony, following unbundling. There is no reason to think that interoperation of data sets would be any different. A consumer might legitimately ask, why is innovation not being given more weight, when it is so important to my welfare? No consumers have access to a product until it is created, and stasis does not serve their interests — unlike corporatist producers. Yet when it comes to data, a powerful stasis bias has been created in favor of those with vertically integrated systems and existing data troves.

Allowing interoperability so as to serve the consumer is important because the static account of data privacy can support significant regulation, raising barriers to entry. Regulators and legislators should not be taken at face value on this point, as they will have their own agendas (notably, budgetary growth) which do not necessarily align with those of consumers or wider society. Indeed, rent seeking under the GDPR may be the answer to the riddles in the curiously broad definitions chosen: the broadest test creates the largest compliance function. The EU's appetite for the GDPR may thus partially be explained: like agricultural policies, fishing quotas, or anti-dumping tariffs, there is scope for negotiators to trade the resulting economic rents. Unfortunately for the consumer, this prioritizes state interests over those of the consumer. This is where consumer-friendly law has an essential role: constraining political entrepreneurship by limiting state action, so as to liberate the market. By contrast, a bureaucratic discretion to define "legitimate" data operability as in Art 6(1)(f) is ripe for rent-seeking, as it creates concentrated benefits and diffuse costs.[22]

---

20 UK Information Commissioner's Office, *Guidance on the use of cookies and similar technologies [under the Privacy and Electronic Communications Regulations],* "What are first party and third party cookies?"

21 Edmund Phelps, *Mass Flourishing*, p.32 (Princeton Univ. Press, 2006).

22 J. Buchanan & G. Tullock, *The Calculus of Consent* (Michigan Univ. Press, 1962).

VI. CONCLUSION: ANTITRUST CONCEPTS TO THE RESCUE?

Competition law used to apply form-based reasoning that might once have regulated interactions in the ice cream parlor: e.g. access to the freezer on the questionable assumption that entry in a neighboring commercial unit is impossible. More recent law looks to the effects from practices rather than their form, applying a consumer welfare test so as to exclude potential rent-seeking in the definition of "public interest."[23] Happily, very recent thought leadership in data protection appears to be more sensitive to the consumer. The UK ICO/CMA joint statement suggests that antitrust enforcers can work with information regulators to develop a pro-consumer approach:

- The UK data protection regulator has published a joint statement with the competition authority, setting out an approach under which competition supports data protection. For example, paragraph 51 states that " 'take it or leave it' terms regarding the use of personal data [are] particularly acute where the platform has market power, such that the user has no meaningful choice but to accept the terms."[24] This is an interesting reinterpretation of the UK Data Protection Act 2018, passed during EU membership, but now open for reconsideration following British independence: is a market power gateway to be applied? If so — cue applause from the competition bar.

- Likewise, paragraph 9 firmly rejects the first party/third party distinction, which had already been removed from GDPR, but was still applied de facto because informed consent is difficult to show in data interoperation. Instead, the ICO notes that "whether information is personal data depends on whether it relates to an identified or identifiable individual." No ifs, no buts, no "in particular… [vague laundry list]" as in GDPR. A major risk-based gateway is being reasserted.

- The most remarkable point is very well-hidden: see fn 16, which defines *loss* from data abuse: "These harms can be wide-ranging and include individual tangible harms such as financial or bodily harm, or the cost of avoiding or mitigating harm; individual intangible harms such as discrimination, unwarranted intrusion, misuse of personal information, or loss of control of personal data; and societal harms such as loss of trust, damage to the rule of law or democracy." This may be the start of a move towards a more robust definition of loss, so as to define harm, and supports the statement that the document seeks a "risk-based approach."[25]

- Paragraphs 50-63 set out consumer-centric definitions of harm, notably admitting that switching may discipline privacy practices: implicitly, if switching is undertaken by a portion of the market, the argument can be made that the remainder choosing *not* to switch is evidence of consumer benefit to those users.

- The statement specifically flags the need to enable data interoperation at paragraph 62: "Data sharing that engenders trust in how personal data is being used is a driver of innovation, competition, economic growth and greater choice for consumers and citizens."

The statement stops short of changing some of the most restrictive rules,[26] but signals a significant change in emphasis. Those steeped in antitrust history may recall similar changes to the definition of core terms, including "significant lessening of competition," "monopolization," and "abuse of dominance." Form-based approaches were changed without changing the letter of the law. Bringing the right cases, rather than changing the law, showed that the law was capable of redefinition to suit developments in economic thought and skepticism as to the benefits of regulation to society at large, unless specific evidence of harm to consumers could be shown.[27] Will the same happen to data protection law? The cause of interoperability appears to be intertwined with the application of a consumer welfare standard to data protection law.

23 See especially UK CMA, "Single-wrapped impulse ice cream: suspected anti-competitive conduct," case closure of 10 August 2017, finding no grounds for action applying contemporary antitrust principles to allegations of exclusionary discounting.

24 I am grateful to Maria Constantin for the insights into the CMA/ICO joint statement and the changes from the *status quo ante*.

25 ICO/CMA joint statement, Para 39 and fn 16.

26 Most prominently, the Privacy and Electronic Communications Regulations: see above fn.17.

27 The classic example is *U.S. v. General Dynamics Corp.*, 415 U.S. 486 (1974), the appropriately named case integrating dynamic analysis into merger control without changing the letter of the law.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.