"A ROSE BY ANY OTHER UNIQUE IDENTIFIER": REGULATING CONSUMER DATA TRACKING AND ANONYMISATION CLAIMS

BY
KATHARINE KEMP

Senior Lecturer, UNSW Faculty of Law & Justice. I am grateful to Nicholas Felstead for Research Assistance.

TechREG CHRONICLE
AUGUST 2022

TechREG Talks...
...with Katharine Kemp, Philip Marsden & Jacqueline Downes

THE SOFTWARIZATION OF REGULATED NETWORK INDUSTRIES AND ITS CONSEQUENCES FOR COSTS AND COMPETITION
By Martin Cave

"A ROSE BY ANY OTHER UNIQUE IDENTIFIER": REGULATING CONSUMER DATA TRACKING AND ANONYMISATION CLAIMS
By Katharine Kemp

THE CASE FOR STRINGENT REGULATIONS OF STABLECOINS
By David S. Evans

CONVERGING PROPOSALS FOR PLATFORM REGULATION IN CHINA, THE EU, AND U.S.: COMPARISON AND COMMENTARY
By Liyang Hou & Shuai Han

WHY REGULATION OF DARK PATTERNS IS HERE TO STAY
By Mihir Kshirsagar

Visit **www.competitionpolicyinternational.com** for access to these articles and more!

"A ROSE BY ANY OTHER UNIQUE IDENTIFIER": REGULATING CONSUMER DATA TRACKING AND ANONYMISATION CLAIMS

By Katharine Kemp

Representations in online privacy policies that certain data is anonymous or "not information that personally identifies you" can have significant consequences. They may indicate that the firm considers the data to be outside the scope of data protection regulation, and/or give consumers the impression that this is data which cannot have an impact on the individual; for example, that it will not add to the individual consumer's profile. However, there are a growing range of data practices and services offered by adtech and data analytics providers that do affect individuals' privacy while claiming not to use personal information, including persistent unique identifiers, data matching using hashed emails and other "identity resolution" services – practices which are not within most consumers' knowledge or understanding. Obfuscation about such activities may not only mislead consumers, but hinder competition on privacy quality by firms that seek to compete on the basis of genuinely privacy-enhancing features. This article argues that claims of anonymization and pseudonymization require tighter regulation under data protection law and should also be rigorously scrutinized under consumer protection law for potential misleading conduct.

01
INTRODUCTION

Representations in online privacy policies that certain data is anonymous or "not information that personally identifies you" can have significant consequences. They may indicate that the firm considers the data to be outside the scope of data protection regulation, and/or give consumers the impression that this is data which cannot have an impact on the individual; for example, that it will not add to the individual consumer's profile.

However, there are a growing range of data practices and services offered by adtech and data analytics providers that do affect individuals' privacy while claiming not to use personal information. These include the development of persistent unique identifiers, data matching using hashed emails and other "identity resolution" services – practices which are not within most consumers' knowledge or understanding.

Applying another identifier to individual consumers ("O, be some other name!") does not overcome the reality that these practices are designed to track and influence the behavior of an individual person, no matter the label ("Thou art thyself").

Obfuscation about such activities may not only mislead consumers, but hinder competition on privacy quality by firms that seek to compete on the basis of genuinely privacy-enhancing features. This article argues that claims of anonymization and pseudonymization require tighter regulation under data protection law and should also be rigorously scrutinized under consumer protection law for potential misleading conduct.

02
"BLANK CHEQUE" PRIVACY POLICIES

It is often said that consumers pay for most digital services with their personal data and attention to advertisements. The personal-data price is essentially set by the supplier in its privacy policy. This may be the main price in the case of some "free" apps and online services, or an additional price where consumers pay a monetary amount for a product or subscription but are also required to accept extra collection and uses of their personal data.

The problems with this method of payment run deep. If privacy policies set the personal-data price, many suppliers are in fact requiring consumers to sign a blank cheque. Privacy terms tend not to set any clear limits on the types of extra and unnecessary personal data that may be collected from or shared with third parties, or the extent of monitoring of the consumer's activities on other apps or websites or offline, or extra commercial and even political purposes for which the consumer's data may be used.

If privacy terms set the price, they also allow the supplier to unilaterally increase that price long after the actual transaction with the consumer, as suppliers reserve the right to sell the dataset as part of an asset or business sale and amend the privacy terms without limitation.

There are currently a number of high-profile cases and campaigns which challenge the legality of the personal-data price charged by digital platforms. Johnny Ryan has long advocated against the lack of purpose limitation in Google's data terms. Liza Lovdahl Gormsen and the Bundeskartellamt have framed Facebook's data practices as abuses of dominance.

There is another common theme in suppliers' representations about consumer data practices that deserves our attention. Privacy terms often state that certain data is "anonymous" or does not include the consumer's name or contact details, and may even specify that the supplier can use this data in any manner "as it sees fit."

The implication is that these data practices cannot affect the individual's privacy. At the same time, many publishers, data brokers and adtech providers tell a very different story to advertising customers, emphasizing their ability to track and influence the activities of millions of individual consumers without reference to their name or email, in some cases even where the consumer has expressly opted out of tracking or identification.[2]

2 As explained in Katharine Kemp, 'How to track consumers who don't want to be tracked: Examples from Australia's largest media companies and their suppliers' (Presentation to ACCC National Consumer Congress, June 16, 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4141609.

03

PRIVACY POLICY REPRESENTATIONS: "NOT YOUR NAME OR EMAIL"

Firms commonly make representations in online privacy policies that certain data the firm uses is "anonymous" or "pseudonymous" or does not "personally identify" the individual (for present purposes, collectively, "anonymous data" claims). The reason for including such claims appears to be two-fold. First, most data protection regulations only apply to "personal information" of some description:[3] firms may argue that the information in question is not "personal" and therefore not subject to the obligations imposed by the regulation. Second, such representations may suggest to consumers that the relevant data practice does not have any impact on their privacy.

For example, Amazon Australia promises consumers that:

> [W]e do not associate your interactions on unaffiliated sites with information which on its own identifies you, such as name or email address, and we do not provide any such information to advertisers or to third-party sites that display our interest-based ads.[4]

Google emphasizes to consumers that, in its exchanges of data with advertising customers:

> We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to.[5]

Similarly, Yahoo tells users it only discloses limited data to advertising customers and data analytics companies:

> We do not share personally identifiable information (like phone number or email address) with these partners, such as publishers, advertisers, ad agencies, or analytics partners.[6]

News Corp Australia informs online readers of *The Australian* newspaper that:

> We may also supplement this collected information with information collected from other trusted businesses with whom you also have a relationship or from public sources. All of this is anonymous information (unless we collect it when you are logged in as a recognisable registered user) …[7]

While these representations are expressed in various ways, the common theme is that they emphasize the data practice does not involve the consumer's name, email, or other contact details. The implication appears to be that it is only data associated with these contact details that could concern the consumer. In turn, the firm's reassurance that these details are not included implies there is little or no impact on the consumer's privacy and makes it less likely that consumers will object to the practice.

04

UNIQUE IDENTIFIERS, HASHED EMAILS, AND IDENTITY RESOLUTION

Such privacy policies tend not to describe for consumers how the firm exchanges information relating to the consumer with advertisers, data analysts and other firms where that information is not labelled with the consumer's name or email address. Yet there are a growing number of such data practices discussed and advertised in the marketing press, which most consumers will never see.

3 In Australia, e.g. the *Privacy Act 1988* (Cth) ("*Privacy Act*") only applies to "personal information" as defined in section 6 of the Act.

4 Amazon Australia, "Interest-Based Ads" (Web Page) https://www.amazon.com.au/gp/help/customer/display.html?nodeId=202075050&ref_=footer_iba.

5 Google, "Privacy Policy" (Web Page) https://policies.google.com/privacy?hl=en-US.

6 Yahoo!, "Welcome to the Yahoo Privacy Policy" (Web Page, April 2022) https://legal.yahoo.com/us/en/yahoo/privacy/index.html. See also BuzzFeed, "BuzzFeed's Privacy Policy and Cookie Policy" (Web Page, June 22, 2022) https://www.buzzfeed.com/about/privacy, referring to "[d]ata that indirectly identifies you such as your IP address, mobile device ID and location data. This data does not include anything that allows us to identify you by name or contact details."

7 News Corp Australia, "Data Usage Policy," *Privacy Centre* (Web Page, August 25, 2020) https://preferences.news.com.au/data.

For instance, various firms have developed **unique identifiers** to track consumers' activities across different websites and apps, even where the consumer does not disclose their email address or login as a user for a particular visit. For example, while News Corp Australia tells consumers that various types of data are "anonymous" if the consumer is not logged in, it tells advertisers that it identifies 16 million consumers using unique identifiers (apparently, a string of numbers) which attaches to the individual consumer's activity even when they are not logged in.[8]

The impetus to develop unique identifiers has increased following changes – and announcements of impending changes – to browsers which no longer support tracking of consumers via third-party cookies. There is a particular drive for a unique identifier to become the common standard so that consumers' online and offline activities can be tracked and combined as pervasively as possible.[9]

Firms also commonly engage in **data matching using hashed email addresses**. For instance, firm A and firm B may each have databases of information concerning their own individual customers and wish to obtain further information about their customers' attributes and activities, without asking the individual customer for that information. One way firm A and firm B can achieve this is by each applying the same hashing algorithm to all email addresses in their respective customer databases, and exchanging data on relevant individual customers when the resulting hashed versions of the email addresses match.[10]

> *Firms also commonly engage in data matching using hashed email addresses*

By using hashed email addresses, firms avoid broadcasting their entire customer database, including names and contact details, to other firms. Nonetheless, following a successful match of the hashed versions of the email addresses, firm A and firm B each collect further information about the individual consumer from the other firm to add to their profile on that consumer, even though the consumer did not disclose that information themselves and has not received notice of the actual exchange.

These processes of hashing email addresses or applying unique identifiers might explain some firms' representations that certain information is "pseudonymous." For example, Amazon Australia states in the later passages of its Interest-Based Ads Notice that:

Some third parties may provide us pseudonymized information about you (such as demographic information or sites where you have been shown ads) from offline and online sources …[11]

No further information is offered as to how this is achieved.

Some firms also offer other **"identity resolution"** services which seek to connect various identifiers that relate to an individual consumer across different transactions, devices, and websites (which is sometimes then tied to a new unique identifier). Identity resolution might be used across different departments dealing with the same customer within the one firm. But it has also been used to connect information about a consumer's activities across different websites, apps, devices, and email addresses, even where the consumer has actively opted out of identifying themselves with a consistent identifier.

The location data company, Near, for example, outlines the following unusual logic:

- Consumers' activities have generally been identified and tracked through an advertising identifier on their mobile phone;
- Changes to Apple's operating system mean that Apple iPhone users can now opt out of this tracking by refusing access to their advertising identifier;
- Many Apple iPhone users have in fact opted out of this tracking and made their advertising identifier unavailable;

8 As per News Connect "Customer Match" promotional video narration, available at https://www.newscorpaustralia.com/growth-stories/discover-new-digital-solutions-to-get-customers-to-notice-want-and-buy-your-brand/.

9 See 'Mi3 Special Report: Australia post-cookies, post-privacy: Implications for brands, publishers and media supply chain' (Mi3, November 2021) https://www.mi-3.com.au/23-11-2021/australia-post-privacy-post-cookies-how-marketers-major-publishes-and-media-supply-0.

10 If the same hashing function is applied to the same email address, it always results in an identical string of numbers and letters unrecognisable to humans, making for highly accurate matching across databases.

11 Amazon Australia, "Interest-Based Ads" (Web Page) https://www.amazon.com.au/gp/help/customer/display.html?nodeId=202075050&ref_=footer_iba.

- There is therefore a "need" for an alternative means of identifying and tracking these consumers.[12]

Accordingly, Near developed a method of identifying the individual behind a device using over 27 signals from their various digital devices which can still be collected, even after the individual has refused access to their identifier.

These practices demonstrate that there are various methods of tracking the activities of an individual consumer – and combining data about an individual consumer's attributes and activities across organizations – without any reference to the consumer's legal name or contact details.

Further, these tracking and identification methods are generally hidden from consumers who do not actively opt into the unique identifier (and may even believe that they have successfully opted out of identification) and have no information about the complex processes by which firms disclose and collect data about the consumer "behind the scenes."

05 MEANING OF "ANONYMOUS," "PSEUDONYMOUS," AND "DE-IDENTIFIED"

Given that individual tracking, data combination and influence are possible in these ways, one might ask whether the data in question is in fact properly classified as "personal information" and therefore subject to existing data protection legislation. The answer to this question will vary across jurisdictions.

A. United Kingdom

Like most data protection regulations, the law in the United Kingdom does not refer to "anonymous information" in its operative provisions. However, recital 26 of the UK General Data Protection Regulation does explain that the GDPR does not apply to "anonymous information" which is "information which does not relate to any identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

The UK Information Commissioner's Office has also explained in its guidance the high standard of irreversible de-identification necessary to render information anonymous:

> Anonymisation means that individuals are not identifiable and cannot be reidentified by any means reasonably likely to be used (i.e. the risk of reidentification is sufficiently remote). Anonymous information is not personal data and data protection law does not apply. Pseudonymization means that individuals are not identifiable from the dataset itself, but can be identified by referring to other information held separately. Pseudonymous data is therefore still personal data and data protection law applies.[13]

This provides some clarity on standards for the anonymization and pseudonymization of information: the latter is classified as personal information while the former is not.

B. California

The *California Consumer Privacy Act of 2018* provides definitions of some relevant terms. For example, the extensive definition of "personal information" – information that identifies, relates to, or could reasonably be linked with a consumer or household – specifically includes IP addresses, unique personal identifiers and inferences drawn from information to create a consumer preference profile.[14] This is supported by definitions of "deidentified" and "pseudonymized" information.

Information is "deidentified" where it:

> cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer

12 Near, "Understanding Apple's App Tracking Transparency Framework and Its Impact on the Ad Ecosystem" (Blog Post, July 12, 2021) https://blog.near.com/marketing-advertising/apples-app-tracking-impact-on-the-ad-ecosystem/; *US Patent No 10979848*, filed on January 5, 2021 (Issued on 13 April 2021) https://patents.google.com/patent/US10979848B1/.

13 Information Commissioner's Office (UK), *Introduction to Anonymisation: Anonymisation, Pseudonymisation, and Privacy Enhancing Technologies* (Draft Guidance, May 2021) https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf.

14 Cal Civil Code § 1798.140(o)(1) (West 2020). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

with added requirements that a business using that information has implemented safeguards that prohibit reidentification; has implemented business processes that specifically prohibit reidentification and prevent inadvertent release of deidentified information; and makes no attempt to reidentify the information.[15]

The Californian definition of "pseudonymization" is similar to that put forward in the UK, emphasizing the need to separate additional information which would make the consumer identifiable:

> 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.[16]

Pseudonymous information generally remains subject to the same obligations as other personal information, as opposed to deidentified information which is exempt. However, the Californian legislation does not make any separate reference to "anonymous" information.

> ***Firms also commonly engage in data matching using hashed email addresses***

C. Australia

In other jurisdictions, there is less clarity. In Australia, for example, "personal information" is defined with reference to whether information is "*about* an identified individual, or an individual who is reasonably identifiable."[17] Personal information is deemed to be "de-identified" if "the information is no longer about an identifiable individual or an individual who is reasonably identifiable."[18]

However, based on the Australian case law to date, it is unclear to what extent a court will consider that technical information such as IP addresses, browser information and device identifiers is "about" an individual and therefore "personal information."[19] Further, there is no definition of "anonymous" or "pseudonymous" information under the Australian statute, and no clear and binding rules concerning how such information should be treated.

In response to the Australian Competition and Consumer Commission's *Digital Platforms Inquiry* recommendations for privacy reform,[20] the Australian Government has undertaken a major review of the *Privacy Act*,[21] leading so far to recommendations by the Attorney-General's Department in its 2021 Discussion Paper.[22]

The Discussion Paper recognizes that the current definition of "personal information" is "somewhat unclear" in its application to technical information.[23] It proposes broadening the definition to refer to information that "relates to" an individual rather than being "about" an individual,[24] more closely aligning the Australian definition with the GDPR definition of "personal data" and likely clarifying that the concept includes technical information used to track the individual's activities.

15 *Ibid* § 1798.140(h) (West 2020).

16 *Ibid* § 1798.140(r) (West 2020).

17 *Privacy Act 1988* (Cth) s 6 (definition of "personal information") (emphasis added).

18 *Ibid* (definition of "de-identified"); OAIC, *Australian Privacy Principles Guidelines*, [B.59]-[B.62]; OAIC, 'Deidentification and the Privacy Act' (Web Page, March 21, 2018) https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act.

19 *Privacy Commissioner v. Telstra Corporation Ltd* (2017) 249 FCR 24, 35–7 [59]– [65] (Dowsett, Kenny & Edelman JJ).

20 Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (Report, June 2019) Recommendations 16, 17 https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.

21 See generally Attorney-General's Department (Cth), "Review of the Privacy Act 1988" (Web Page) https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988; Australian Government, *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Report, 12 December 2019) 6 https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf.

22 Attorney-General's Department (Cth), *Privacy Act Review* (Discussion Paper, October 2021) https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.

23 Attorney-General's Department (Cth), *Privacy Act Review* (Discussion Paper, October 2021) 21 https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.

24 *Ibid* 26 (Proposal 2).

The Discussion Paper also includes a proposal for requiring that the collection, use or disclosure (collectively, processing) of personal information is "fair and reasonable."[25] This represents a welcome move away from overreliance on a "notice and consent" model that depends on consumers impaired understanding of firms' actual data practices, and would be supported by several legislated factors relevant to determining whether processing is fair and reasonable in the circumstances.[26]

06

BEYOND DEFINITIONS: TRANSPARENCY AND ACCURACY

However, even clearer definitions of terms such as "anonymous," "pseudonymous," and "de-identified" will not be a complete solution to the kinds of representations raised in this article. As evident in the examples listed above, firms already choose to use other, vaguer terminology to describe the relevant data, such as "not information which on its own identifies you."

With this nebulous wording, consumers are not only left in the dark about the extent to which the data practice will affect their individual privacy, but often cannot tell whether the firm is claiming that such information is outside the scope of the data protection regulation, or that it is within the scope of the data protection regulation and, if so, for what specific purposes the firm proposes to use it.

Such uncertainty is unacceptable when firms are obliged to provide individuals with transparent and accurate information about their data practices. If the firm accepts that the information is personal information, there is a strong argument that qualifications about the absence of names and contact details should not be permitted to muddy the waters and obscure the substance of the data practice. If the firm claims the information is not personal information, it should make clear the basis for this claim: the absence of a name or contact details will not be sufficient.

07

SCRUTINY UNDER CONSUMER PROTECTION REGULATION

Consumer protection law also has a vital role to play in regulating representations about anonymization and methods of tracking in the meantime. Importantly, under consumer protection laws, a court is not constrained to consider whether certain mandated disclosures have been made in the fine print of a privacy policy, but must consider whether the firm's conduct as a whole creates an impression that misleads, or is likely to mislead, consumers about the nature of their data practices, having regard to consumers' likely level of information and comprehension.

We should not proceed on the unrealistic assumption that a consumer will be capable of unravelling the semantic intricacies of the fine print on the fifth page of a privacy policy. The realistic capacity of the reasonable consumer must be taken into account. This is reflected in the reasoning of the Federal Court of Australia in the *Google Location Data case*,[27] where Thawley J acknowledged that there are limits to the trouble that reasonable users would take to arrive at an accurate understanding of a firm's data practices, even for consumers who are concerned about their privacy.[28] Thus his Honor noted that "[t]here is a point where reasonable people give up drilling down to plumb the depths of further information."[29]

Similarly, in proceedings arising out of Facebook's data policies and the Cambridge Analytica scandal, a court in the United States noted the obstacles to comprehension for those reading Facebook's contractual language: "it would have been difficult to isolate and understand the

25 Attorney-General's Department (Cth), *Privacy Act Review* (Discussion Paper, October 2021) 85 (Proposal 10.1).

26 Attorney-General's Department (Cth), *Privacy Act Review* (Discussion Paper, October 2021) 89 (Proposal 10.2).

27 *Australian Competition and Consumer Commission v Google LLC [No 2]* (2021) 391 ALR 346.

28 *ACCC v Google LLC (No 2)* [2021] FCA 367, para 210.

29 Ibid 389 [210].

pertinent language among all of Facebook's complicated disclosures."[30]

In the present context, consumer protection regulators should consider whether a given "anonymous data" representation is likely to create the false impression that:

- the relevant data exchange can add no further information to the firm's collection of data about the consumer as an individual,
- the consumer's relevant activities will not later be associated with any profile that identifies the consumer or the consumer's device, or
- the information in question cannot be used to determine what communications and offers will be displayed on the individual consumer's device based on their specific attributes and activities.

We should also question whether it is appropriate to use terms such as "pseudonymous" which may have absolutely no meaning for the average consumer and serve only to confuse. There is a need for research to determine consumers' understanding of these terms and representations, and therefore the risks created by their use.

08

HINDERING COMPETITION ON PRIVACY QUALITY

The lack of transparency and choice regarding these practices has significance beyond the question of compliance with data protection and consumer protection regulation. Obfuscation about the nature of these practices is also likely to hinder firms who seek to compete on the basis of superior privacy quality.

Consider a search engine that competes on the basis of privacy-enhancing features, abstaining from collecting any personal information. Such a supplier will not be able to make these advantages as salient to consumers seeking improved privacy if the privacy-degrading features of its rivals' services can be concealed in vague representations that certain data does not personally identify users.

Adtech providers who innovate with business models – including innovative contextual advertising models[31] – that do not depend on tracking consumer behavior, will also be disadvantaged. These representations prevent consumers from making a comparison between the privacy-enhancing approach to advertising of these providers and the privacy-degrading approach to advertising of those who pervasively monitor consumer behavior and combine personal data across multitudes of businesses to create a "360-degree view" of consumer that allows their behavior to be predicted and manipulated.

In most cases, this hindrance of competition due to the conduct of any given firm is unlikely to amount to an antitrust contravention. Practices would be more likely to fall foul of competition laws where rivals coordinate their activities: for example, if rival firms adopt a common identifier to track individual consumers across their respective sites, apps, and services subject to the same terms and representations. More generally, competition policy depends on adequate consumer protection regulation and enforcement to ensure that consumers have the information necessary to select products according to their true preferences.

09

CONCLUSION

Firms should not be permitted to make confusing and potentially misleading representations about data practices that do not include consumers' names and contact details. Many firms are aware that the absence of such details does not prevent their data practices – such as data matching, unique identifiers, and identity resolution – from intruding upon the individual consumer's privacy. In the circumstances, these "anonymous data" representations prevent consumers from making accurate comparisons of data terms and impair effective competition on privacy quality by firms who innovate to enhance privacy.

To comply with their data protection obligations to provide transparent and accurate information on their data handling, firms should only make "anonymous data" representations if they clearly articulate their claim that the data is not personal data under the relevant regulation and the basis for this claim. Consumer protection regula-

30 *Re Facebook Inc*, 402 F Supp 3d 767, 792 [17] (Chhabria J) (ND Cal, 2019).

31 See e.g. Greens EFA, "The future of advertising: Innovative practices on the rise" (April 19, 2022) https://www.youtube.com/watch?v=17aZdbFLGIA.

tors should also scrutinize such representations to determine whether the firm's conduct is likely to mislead consumers about the true nature of the firm's data practices.

> *In most cases, this hindrance of competition due to the conduct of any given firm is unlikely to amount to an antitrust contravention*

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.

CPI COMPETITION POLICY™ INTERNATIONAL