PLATFORM POWER AND PRIVACY PROTECTION: A CASE FOR POLICY INNOVATION

BY CARON BEATON-WELLS[1]

1 Professor of Competition Law, University of Melbourne; Host, Competition Lore podcast on competition in a digital age. This article represents early exploratory thinking. Comments and feedback most welcome. Contact c.beaton-wells@unimelb.edu.au.

CPI ANTITRUST CHRONICLE
SEPTEMBER 2018

CPI Antitrust Chronicle August 2018

www.competitionpolicyinternational.com

I. INTRODUCTION

Antitrust debates regarding competition in data-driven markets, particularly those dominated by digital platforms, have run headlong into issues of privacy. This was inevitable.

At the heart of the platform business model is the collection and use, for commercial gain, of unfathomably large amounts of personal information. Such information is the *sine qua non* of privacy concerns.[2] Given their increasing power as information gate-keepers and intermediaries across swathes of the digital economy, it is barely surprising that platforms find themselves in the line of fire for modern-day privacy concerns.

Public engagement with, and intellectual discourse on, the intersections between antitrust and privacy policies have been fueled by the Cambridge Analytica scandal. As an episode that saw the harvesting of personal information from millions of Facebook users for the purposes of electoral manipulation, it pushed the power of platforms and privacy protection, along with their political implications, onto front pages around the world.

Much of the antitrust debate surrounding privacy has been focused on whether and how to nest[3] privacy into antitrust. Broadly speaking, the debate appears divided between two camps.

In one corner are those who see complementarities or synergies between antitrust and privacy policy goals. This is a view premised on a broad conception of antitrust, most commonly associated with doctrine in the European Union ("EU"), but also with the so-called "New" or "Neo-Brandeis" school that has emerged in the U.S.[4] It is underpinned by a commitment to state intervention for the promotion of pluralist aims of antitrust, including those of a political and social orientation, not just an economic one.

In the other corner are those who regard antitrust and privacy as largely occupying different and disconnected policy terrains. This is a view

2 That said, as a concept, "privacy" extends beyond a concern with keeping personal information private (it extends to behavioral privacy for example). It is also notoriously difficult to define and varies according to time and place. See e.g. Robert C. Post, *Three Concepts of Privacy*, 89 GEO L.J. 2087 (2001).

3 James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, The First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129 (2013).

4 See Lina Khan, *The New Brandeis Movement: America's Antimonopoly Debate*, 9(3) J. Euro Comp L. & P. 131 (2018). Further, see the collection of articles in *Hipster Antitrust*, Antitrust Chronicle, COMPETITION POLICY INTERNATIONAL (April 2018). There may be some irony in the fact that, based on his concerns about the effects of concentrated economic power on a free society, this school takes its name after the same former U.S. legal scholar and Supreme Court associate justice who co-authored the seminal article on privacy, capturing essential tenets of that right as reflected in European privacy doctrine (see further below): Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4(5) HARVARD L.R. 193 (1890).

premised on a narrower conception of antitrust, generally associated with the approach promulgated by the Chicago school, particularly in the U.S.[5] It is underpinned by a commitment to self-correcting markets in the singular pursuit of economic efficiencies that serve consumer welfare.

In analyzing the antitrust-privacy interface, it may be useful to distinguish between these two approaches by reference to a model of policy consistency on the one hand and a model of policy separation on the other. Both have their limitations. A separatist model, promoting regulatory silos, risks conflict between antitrust and privacy policies in dealing with personal information or consumer data. In particular, strengthened privacy protection may undermine competitive forces.[6] A consistency model, promoting regulatory integration, may reduce this conflict. However, it risks being at the expense of policy experimentation as policymakers remain bound by entrenched frameworks that fail to realize the potential of data in a digital economy.[7]

Part II of this article maps the contours of these two models, as they are played out in arguments concerning whether and how to embed privacy within antitrust. Part III explains how these approaches relate to differences in the underlying values associated with privacy and antitrust, and points to the relevant legal and institutional frameworks in the EU and the U.S. as reflecting those values. Part IV proposes a third way, a model based on policy innovation, exemplified by Australia's introduction of a comprehensive consumer right to data. Part V briefly concludes the argument.

II. POLICY CONSISTENCY VS POLICY SEPARATION

There are various arguments that have been made in support of incorporating privacy into antitrust analysis reflecting a model of policy consistency.[8] One of these involves treating privacy as a non-price element of competition. This characterization allows for privacy degradation to be treated as a reduction in quality and, on that basis, as harmful to consumers notwithstanding that, in many instances, prices (at least in monetary terms) for platform services are zero. In addition, information asymmetries between data subjects and data holders are a matter for concern on the grounds that they may facilitate consumer exploitation as well as price and, conceivably, behavioral discrimination. In turn, such discrimination is pointed to as aggravating inequality, which for some falls within the compass of antitrust-related concerns. More broadly there is general acceptance of the view that, at a certain scale, data and its uses are a source of market power that may foreclose entry. Economies of scale and network effects are key in this analysis. However, concerns are not limited to the economic implications of power in markets. The political, social, and cultural impact of so-called "data-opolies" is at issue too, and greater privacy protection (with its attendant restrictions on data extraction and mining) is identified as having the potential to ameliorate such impact.

5 See e.g. Richard Posner, *The Chicago School of Antitrust Analysis*, 127 U. Pa. L. Rev. 925 (1979).

6 An effect being identified in relation to the General Data Protection Regulation introduced in Europe in May 2018. See e.g. Daniel Lyons, *GDPR: Privacy as Europe's tariff by other means?*, AEI IDEAS (Jul 3, 2018), http://www.aei.org/publication/gdpr-privacy-as-europes-tariff-by-other-means/.

7 While beyond the scope of this article, the adoption of different models across jurisdictions also has implications for international data trade. See Filippo Maria Lancieri, *Antitrust Enforcement in Big Data Markets: What is the role of privacy and antitrust cultures?*, (Jan 2017), https://www.researchgate.net/publication/321638142_Antitrust_Enforcement_in_Big_Data_Markets_What_is_the_Role_of_Privacy_and_Antitrust_Cultures. There are additional related questions regarding processes of global policy convergence. See e.g. Colin J. Bennett, *The European General Data Protection Regulation: An instrument for the globalization of privacy standards?*, 23 INFORMATION POLITY 239 (2018).

8 For a representative sample of sources for such arguments, see Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 2 GEO. L. TECH. REV. 275 (2018); Peter Swire, "Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall," (Oct 18, 2007), https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis/; Pamela Harbour & Tara Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, (2010) Antitrust L.J. 769-97; Wolfgang Kerber, *Digital markets, data, and privacy: competition law, consumer law and data protection*, 11 J. Intell. Prop. L. & Pract. 856 (2016); Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 850, http://open.wmitchell.edu/cgi/viewcontent.cgi?article=1568&context=wmlr; Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009 (2013).

In contrast, consistent with a model of policy separation, the relevance of privacy concerns in the antitrust arena is resisted while issues associated with the operationalization of privacy in an antitrust context are raised also.[9] While conceding some merit to the argument that privacy may be characterized as a non-price (quality) element of competition, challenges are identified in relation to measuring quality effects and making trade-offs between data extraction at the expense of privacy and targeted advertising (or even innovation more broadly) to the benefit of consumers. While not necessarily discounting information asymmetry as a consumer protection concern, exploitation and discrimination are seen to be outside the purview of legitimate antitrust harm theories. Foreclosure arguments are discounted on the grounds that data is non-rivalrous, and consumers multi-home. Moreover, cases of successful new platform entry (as well as cases of failure) over time are routinely pointed to as evidence against data facilitating unassailable competitive advantage. More generally, it is argued that allowing antitrust enforcers to consider privacy would inject an undesirable level of subjectivity into enforcement decisions. Risks of false-positives and the associated chilling of innovation are often articulated in this line of reasoning. Relatedly, based on the view that privacy is fundamentally a non-competition concern it is seen as a matter for legislatures, not antitrust agencies and courts.

The divergence in these approaches may be better understood if we appreciate that they reflect underlying differences not just in the way antitrust goals are conceived, but in the way privacy goals are conceived as well. Looking beyond the technocratic arguments, it appears that the divide lies ultimately between the view that antitrust and privacy share basic foundational values and the view that they are founded on values that are quite separate and distinct.[10]

The point is most readily made by contrasting EU and U.S. values as they relate to power in the context of both antitrust and privacy, and is borne out by an examination of the legal and institutional manifestations of those values.

III. THE ANTITRUST-PRIVACY INTERFACE: A QUESTION OF VALUES

In a model of policy consistency, most prominently displayed in Europe, power in and of itself is a problem that warrants intervention, whether in the context of privacy or antitrust.

Through a privacy lens, this is because privacy violations are regarded as violations of personal dignity, respect, and autonomy or self-determinism, concerns which are deeply rooted in the history of European armed conflicts and the continent's intellectual tradition.[11] Preserving image and reputation in the interests of personal dignity mean that the powers of the free press and the free market have to be curbed. Moreover, as a reaction against hierarchical class structures of earlier centuries, dignity is to be afforded to all members of society regardless of their socio-economic standing.[12] This is a function of values associated with egalitarianism, or comparative fairness.

Through an antitrust lens, in Europe (but also in the U.S. according to the Neo-Brandeisian school), power is problematic for reasons that include its propensity to generate exploitation or unfairness.[13] It follows that attention must be given to market structure as much as to market conduct. In the latter case, consideration may be given to economic efficiency and harm to consumer welfare. However, in the former case, concentration of power is to be curtailed in its incipiency or dismantled *ex-post* not only on economic grounds (so as to remove threats to the competitive process) but also on the grounds that such power spawns inequality and is insidious to the workings of a liberal democratic society.

---

9 For a representative sample of sources for such arguments, see Geoffrey Manne & Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, (2015) 2 ANTITRUST CHRONICLE 3; Samson Esayas, *The Idea of 'Emergent Properties' in Data Privacy: Towards a Holistic Approach*, 25 (2) Int J. L. & T. 139 (2017); D. Daniel Sokol & Roisin Comerford, *Does Antitrust Have a Role to Play in Regulating Big Data?* in Roger Blair & Daniel Sokol (eds), CAMBRIDGE HANDBOOK OF ANTITRUST, INTELLECTUAL PROPERTY AND HIGH TECH (2016); Noah Phillips, *Keep It: Maintaining Competition in the Privacy Debate*, (Remarks for Internet Governance Forum, July 27, 2018), https://www.ftc.gov/public-statements/2018/07/keep-it-maintaining-competition-privacy-debate.

10 In turn these foundational values are derived from fundamental socio-cultural norms shaped by historical experience and political tradition, full discussion of which is beyond the scope of this article. See e.g. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151 (2004).

11 See e.g. Robert Kagan, OF PARADISE AND POWER: AMERICA AND EUROPE IN THE NEW WORLD ORDER 11, 58-62 (2003).

12 James Q. Whitman, *On Nazi 'Honour' and the New European Dignity* in Christian Joerges & Navrak Singh Ghaleigh, DARKER LEGACIES OF LAW IN EUROPE: THE SHADOW OF NATIONAL SOCIALISM AND FASCISM IN EUROPE AND ITS LEGAL TRADITIONS 243, 251-262 (2003).

13 See Ariel Ezrachi, *EU Competition Law Goals and The Digital Economy*, Aug. 8 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191766.

Competition on the merits is not to be "fenced out by power, privilege or favoritism."[14]

It follows that in both the privacy and antitrust spheres, underlying values support a strong role for government in regulating relations between private actors. That much is evident in the relevant legal and institutional frameworks.

In Europe, privacy and data protection enjoy a status as fundamental human rights.[15] These inalienable protections are implemented through a formidable legal framework, as contained most recently in the General Data Protection and Regulation Directive ("GDPR"),[16] and supported by a powerful institutional apparatus.[17] Updating and extending a 1995 Directive, the GDPR enshrines a series of rights for data subjects and imposes significant obligations on data controllers and processors. It establishes a range of accountability and compliance mechanisms and threatens onerous sanctions in the event of breaches.

EU antitrust doctrine applies largely formalistic criteria, as distinct from economic effects or efficiency-based reasoning, in imposing liability on dominant undertakings. It imposes "special responsibilities" on such entities and has socially oriented elements that include bans on "excessive prices" and price discrimination, as well as the view that unfair trading practices may constitute an abuse of a dominant position. Competition authorities in this jurisdiction have a long track record of bringing and defending such cases before the courts and of imposing massive fines, not infrequently accompanied by behavioral and sometimes structural remedies.[18]

In contrast, under a model of policy separation as applies in the U.S., power in and of itself is a concern for privacy but not for antitrust (at least not according to the Chicago school, which may be facing serious challenges but still stands as the basis for antitrust jurisprudence and agency practice over the last 30 years).

In the privacy realm, it is largely the power of the state that is at issue. Such power needs to be restrained so as to prevent unjustified incursions on civil liberties. Suspicion of government authorities and their intrusion into private affairs, into the sanctity of one's own home especially, are the foundation on which much of American privacy doctrine and thinking has been built.[19] Hence the regulatory focus is primarily on relations between public and private actors. Extensions of EU-style privacy into private-private relations face significant obstacles associated with the value of the free market and the value of the free press. If privacy is to be protected in this realm it is largely as a consumer protection measure so as to prevent or ameliorate market failures emanating from information asymmetry.[20]

In the antitrust realm, power *per se* is not problematic given that it may be derived from efficiency. Firms that win market power by virtue of competing effectively are not to be stripped of their rewards for fear of eroding or removing incentives for efficiency, seen as being in the interests of consumer welfare (defined in terms of surplus as distinct from any broader notion of welfare or wellbeing). Rather it is the exercise of market power with the effect of excluding rivals in the absence of any efficiency justification that is of concern. It follows that in this context, but only on limited grounds, state intervention in private-private relations (or the market) may be warranted. Intervention motivated by other concerns, particularly of a fairness or distributive character, are eschewed as misplaced, tantamount to social as distinct from economic policy, and as likely to undermine the coherence and effectiveness of antitrust doctrine.[21]

---

14 Eleanor Fox, *Monopolization and abuse of dominance: Why Europe is different*, 59(1) ANTITRUST BULLETIN 129, 132 (2014).

15 European Convention on Human Rights (art. 8); European Charter of Human Rights (arts 7 & 8).

16 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016.

17 See Paul Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L.REV. 1966 (2013).

18 See generally Pinar Akman, THE CONCEPT OF ABUSE IN EU COMPETITION LAW: LAW AND ECONOMIC APPROACHES (2012).

19 See Jeffrey Rosen, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 5 (2000).

20 See further Julie Brill, *The Intersection Between Consumer Protection and Competition in the New World of Privacy*, 7(1) COMPETITION POLICY INTERNATIONAL (Spring, 2011).

21 See e.g. Mauritz Dolmans & Wanjie Lin, *Fairness and Competition Law: A Fairness Paradox*, CONCURRENCES (No. 4, Nov, 2017), https://www.concurrences.com/en/review/issues/no-4-2017/articles/fairness-and-competition-law-a-fairness-paradox.

Hence, in the case of privacy there appears to be a strong basis for legal protection, but only or predominantly against the state. In the case of antitrust, the argument for legal intervention is much weaker. Again, the underlying values as they relate to power are evident in the relevant legal and institutional frameworks.

The U.S. right to protection from state intrusion into citizens' private lives stems from and has been extended in jurisprudence invoking the Fourth Amendment of the Constitution (enshrining rights against unlawful searches and seizures). Efforts to import privacy protections in private relations from Europe are invariably countered by another fundamental set of rights in the U.S., namely the rights to freedom of speech or of the press, under the First Amendment. In the setting of the free market, information or data is regarded as an asset and hence may be traded as a freely alienable right. Unlike in Europe and many other parts of the world, there is no federal omnibus legislation governing privacy, but rather a mosaic of federal and state statutes and regulators that are sector-, activity-, and/or data-specific.[22] The closest version of a general federal privacy regulator takes the form of the Federal Trade Commission, but its jurisdiction is limited to dealing with privacy as a consumer protection or fair trade issue. Consistent with this mandate, its primary concern has been with systems of notice and consent. It also relies heavily on soft law or co-regulatory approaches, and has no rule-making authority or power to fine.[23]

In antitrust, since the 1970s and under the intellectual hegemony of the Chicago school, a *laissez-faire* attitude to structural concerns has meant that concentration through merger activity has met with minimal resistance. The predominant focus of enforcement has been on so-called hard-core cartels. Faith in markets and business judgment, particularly associated with the pursuit of efficiencies, together with an imperative to avoid false-positives, have resulted in almost absentee enforcement of monopolization claims. Rule of reason tests have been favored over *per se* liability standards in relation to any conduct other than the most obvious horizontal restraints. Price discrimination has been neglected on the basis that it reflects distributive concerns. Consumer harm has been conceptualized predominantly in terms of price effects, and there has been a general insistence on measurability or quantification for the purposes of harm assessment.[24]

As policymaking and associated laws and institutions generally reflect deeply ingrained social and political values and traditions, the EU-U.S. divergence in relation to the antitrust-privacy interface is perhaps not surprising. As models of policy consistency and policy separation, the merits and demerits of each would be open to debate and views inevitably will differ, again reflecting the values underpinning them. However, presenting the two models as a binary choice (as so often is the case in discourse about a transatlantic divide on a wide range of issues) would be a mistake. It would also be a lost opportunity. Is there another way?

IV. POLICY INNOVATION

Recent developments in Australia point to an alternative model, based on policy innovation. The Australian government has proposed introducing a new "Consumer Data Right" ("CDR").[25] It is presented as a policy reform to drive competition and innovation or, even more ambitiously, to advance and secure the future welfare of all Australians in a digital economy.[26] In effect, the reform is concerned with facilitating data portability and transfer to enable consumers to use their data to compare and switch between product and service providers, ensuring that consumers have more information and choice while giving businesses greater incentives and capacity to compete.

22 See Franz-Stefan Gady, *EU/U.S. Approaches to Data Privacy and the 'Brussels Effect': A Comparative Analysis*, Geo J. Int. Affairs 12 (2014).

23 See generally David A. Hyman & William E. Kovacic, *Implementing Privacy Policy: Who Should Do What?* (Feb 13, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3123115.

24 See e.g. Maurice Stucke & Ariel Ezrachi, The Rise, Fall, and Rebirth of the U.S. Antitrust Movement, HARV BUS REV. (Dec 15, 2017); Joshua Wright, *Abandoning Antitrust's Chicago Obsession: The Case for Evidence-Based Antitrust*, 78 ANTITRUST L.J. 301 (2011).

25 See https://treasury.gov.au/consumer-data-right. The proposal is based on recommendations made by the Productivity Commission, *Data Availability and Use*, Inquiry Report (May, 2017), http://www.pc.gov.au/inquiries/completed/data-access/report.

26 In part, the basis for this broader ambition, is that the reform is concerned also with greater sharing and release of public sector data (not discussed in this article). See Australian Government, Department of Prime Minister and Cabinet, *New Australian Government Data Sharing and Release Legislation*, Issues Paper for Consultation (Jul. 4, 2018), https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation.

Similar reforms have been implemented in other countries in specific sectors,[27] and the GDPR, which is economy-wide, also provides for data transfer.[28] However, in aspects of both its substantive provisions and its institutional arrangements, the Australian model is arguably first-of-its-kind. The following facets of the reform are especially noteworthy in this respect:

First, "consumers" are to include not just individuals, but also businesses irrespective of size.

Second, "consumer data" is to be defined broadly, including data that identifies and is identifiable with the consumer, whether provided directly by the consumer, collected in the course of actions taken by the data holder or held by the data holder even if created by others.

Third, the right is essentially that of consumers to have access to and control over their data, enabling them to have it transferred by the data holder to an accredited third party at their direction, and in a form that is digitally practicable.

Fourth, both the nature of the data and the form in which it would be transferable are to be based on an outcomes-focused principle, namely that it should include the data and in the form that a competing business would need in order to make a reasonable offer for the consumer's patronage. Subject to that principle, it is recognized that types of data will vary between sectors and that technological change will affect the nature of data that is generated over time. Hence there will be an industry data-specification process that enables the relevant industry to agree on the types of data that will be covered, as well as mechanisms for transfer and security protocols.

Fifth, the emphasis on creating an inalienable right of control steers (deliberately) away from a right of ownership (a property right), which would be alienable and is arguably nebulous in any event, as it would be practically difficult if not impossible to exercise.[29] Furthermore, it is a right of *joint* control of data as an asset shared by data holders and data subjects, one of the implications of which is that, unlike the GDPR, the CDR does not extend to a right to deletion (the so-called "right to be forgotten"). While sharing control with data holders, data subjects are empowered to limit aspects of data use in ways that may most concern them (for example, on-sale of data without disclosure or consumer consent).

Sixth, the CDR is to apply economy-wide. While this is important in creating incentives for all private enterprises to act on the privacy concerns of consumers, application of the new law is neither automatic nor immediate. Rather, it is recognized that in certain respects the reform is experimental and that there may potentially be significant transition and set up costs. Hence, adopting a scalable risk-based approach, it is to be rolled out sector-by-sector, starting with the banking sector, to be followed by telecommunications and energy. This will not only enable the system to be industry-customized and reduce upfront costs but will facilitate consumer education in one sector that should then be more readily transferable to others, as well as allowing for the policy to be refined as lessons are derived from the implementation experience.

Finally, consistent with competition being its primary rationale, the new regime makes the Australian competition authority, the Australian Competition and Consumer Commission, the lead regulator. The Commission is to have responsibilities over the approval of data-specification agreements and standards, accreditation of data recipients, handling complaints about, and taking enforcement action in response to breaches of the CDR rules. In the event of liability, significant penalties would apply.

At the heart of this model is a basic distinction drawn between privacy and competition as each relates to consumer data. While privacy focuses on managing data use by *others*, the CDR focuses on enabling consumers *themselves* to control its use. In essence, the distinction is between limitation or aversion of a threat (to which privacy policy is directed) and opening up and spreading of opportunity (to which competi-

27 In banking in particular, see e.g. Open Banking Goes Live – What Will it Mean for Consumers? (2018), https://www.consumersinternational.org/news-resources/blog/posts/open-banking-goes-live/.

28 In the U.S., Senate Intelligence Committee Vice Chairman, Mark Warner, has produced a set of policy proposals for regulating large digital platforms which include U.S. adoption of GDPR-style legislation with its right relating to data portability. See Sen Mark R. Warner, *Potential Policy Proposals for Regulation of Social Media and Technology Firms*, White Paper (DRAFT), https://graphics.axios.com/pdf/PlatformPolicyPaper.pdf. Not surprisingly the proposals are attracting much comment, including scathing critique from commentators of the Chicago-persuasion. See e.g. Kristian Stout, Senator Warner's retrogressive proposals could lead to arbitrary and capricious interventions that would harm entrepreneurs and consumers, *Truth On the Market* (Aug. 10, 2018), https://truthonthemarket.com/2018/08/10/senator-warners-retrogressive-proposals-could-lead-to-arbitrary-and-capricious-interventions-that-would-harm-entrepreneurs-and-consumers/.

29 Cf. Luigi Zingales & Guy Rolnik, *A Way to Own your Social Media Data*, New York Times (Jun. 30, 2017), https://www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html. It also steers well clear of debates as to whether consumers should be paid for their data. See e.g. *What if people were paid for their data?*, (Apr., 9, 2018) The Economist, https://medium.com/@the_economist/what-if-people-were-paid-for-their-data-8df63f021e38.

tion policy is directed). Drawing the distinction allows for the narrative surrounding data to be changed, from one concerned with harms to one concerned with benefits.

At the same time, the proposed reform does not alter, or in any way erode, existing protections for personal information under privacy laws in this jurisdiction. Indeed, in several respects, the new right strengthens privacy protections in establishing greater transparency and choice for consumers in controlling how their information will be used, providing for the mandatory accreditation of data recipients, ensuring there are standards for data transfer and security set by a Data Standards Body, allocating a strong role for the Australian privacy regulator in advising on and enforcing privacy protections, and providing a range of avenues for consumers to seek meaningful remedies for breaches, including external dispute resolution and direct rights of action.

In broader terms, the CDR reform is motivated by what is seen as a modern-day imperative for government and private enterprises in a digitally transformed economy, namely to ensure that there is a "social license" for data collection and use. Social license is to be derived from community acceptance and trust in providing data and allowing for its use, to the benefit of the economy and society as a whole.[30] In this sense, the proposed CDR is more than a competition, consumer protection, or even privacy reform. The need to build social license in these areas is based on growing evidence of citizen-consumer distrust in technology generally, in data handling practices specifically, and an associated increasing distrust in societal institutions. This distrust creates a risk for data holders: there will be a tipping point where the balance of willingness tips away from data supply to data restriction and where government steps in to regulate in ways that may too tip the balance towards restriction. Such tipping would be to the detriment of businesses that profit from data collection and use, but also to the detriment of progress and innovation that benefits consumers and the community generally.

The CDR aims to alter this direction, building trust by ensuring that consumers, as the source of the data from which we all benefit, have greater influence over how value is created and extracted from it, as well as ensuring that there are robust institutional and governance arrangements supporting it.[31] The values underpinning and embedded in the model could be characterized as social – shared control and shared benefit – but the outcomes undoubtedly will be economic. Moreover, "the social" and "the economic" will be mutually reinforcing. The trust engendered by greater consumer control over data and confidence in "the system" facilitating this control should contribute to an ongoing support for data-sharing initiatives and active participation by individuals in the data eco-system. If data is shared and used in trusted, protected, and inclusive ways, this will drive even more value that can, in turn, create more trust, inclusion, and control. The full value of data will be unlocked.

V. CONCLUSION

The privacy debate is not a passing fad. As economies and societies continue to be transformed by the data revolution, privacy protections will continue to be paramount, and digital platforms are likely to continue to be a hotbed for such concerns. Policymakers will have to confront pressing questions over how best to protect privacy while at the same time promoting competition.

Policy responses are shaped by societal values. In the EU there is an alignment in the values associated with both competition and privacy, allowing for consistency in policy responses. In the U.S. there is less alignment and, in some respects, misalignment, allowing for potential conflict. Drawing on an innovative Australian model, this article proposes a different approach. Taking a page out of both the U.S. and EU books, it treats privacy concerns as distinct from competition but also recognizes the possibility of policy responses that have positive mutually reinforcing effects on both.

30 See Productivity Commission, *Data Availability and Use*, Inquiry Report (May, 2017), chp 4, 177-178, http://www.pc.gov.au/inquiries/completed/data-access/report.

31 See Productivity Commission, *Data Availability and Use*, Inquiry Report (May, 2017), chp 5, 192, http://www.pc.gov.au/inquiries/completed/data-access/report.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 20,000 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.