University of New South Wales Law Research Series

PERSONAL DATA LAW AND COMPETITION LAW – WHERE IS IT HEADING?

ROBERT WALTERS, BRUNO ZELLER AND LEON TRAKMAN

Forthcoming (2018) 39 *European Competition Law Review*
[2018] *UNSWLRS* 73

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Personal Data Law and Competition Law – where is it heading?

*Dr. Robert Walters,[1] **Professor, Dr. Bruno Zeller, ***Professor, Dr. Leon Trakman

Australia, Competition Law, Data Protection Law, European Union, Singapore

Abstract

Data protection and competition law have different objectives. This paper examines the interconnectedness between these laws, and highlights current examples that have emerged to create a competitive edge. The paper proposes a two stage solution, and compares the European Union, Australia and Singapore.

Key Words Australia, Competition Law, Data Protection Law, European Union, Singapore

Introduction

There are increasingly calls for competition regulators to incorporate the possession of personal data into their analyses of anticompetitive[2] practices and behaviour. The point is that the control of large amounts of both commercial and personal data will give companies an unfair advantage over competitors. It is well settled that in the past commercial data has been used to create anticompetitive practices, which has allowed companies to capture a dominant position. However, it has only recently emerged that personal data is also being used as a tradable commodity that is placing entities in a position whereby they can use the data to bargain for a stronger position in the market, because they have exclusive access to personal data.

At issue is the competing forces between competition and personal data protection law. Competition law specifically looks at the behavior of individuals and organizations with regard to products, choice and price. On the other hand, data protection law has a role in protecting

[1] * Robert Walters LLB (Victoria), MPPM (Monash), PhD Law (Victoria), Lecturer, Victoria Law School, Victoria University, Melbourne, Adjunct Professor, European Faculty of Law, The New University, Slovenia, Europe.

** Bruno Zeller B.Com, B. Ed, Master of International Trade Law (Deakin), PhD (The University of Melbourne). Professor of Transnational Commercial Law, University of Western Australia.

*** Leon Trakman B. Com, LLB (Cape Town); LLM, SJD (Harvard), Professor of Law and Former Dean, Faculty of Law, University of New South Wales, Sydney.

[2] For the purposes of this paper, the terminology of ant-trust and competition mean the same and are used frequently.

the privacy of the individual person's – personal data that has been defined under national or supranational law. This protection has become necessary because large amounts of personal data are being used in anticompetitive behavior.[3] In turn organizations use their market power to take advantage of consumers and competitors.[4] However, it is argued that competition and data protection laws do converge at a conceptual level, because these laws, to varying degrees, provide a level of consumer protection.

Moreover, anti-competitive behavior, from the collection, use and application of personal data can be traced to predominantly two different forms. Hence, two issues emerge the first is the personal data defined by law that is stolen or used without the consent of the data subject to enhance market power by corporations. The second corresponds to situations in which personal data, which is defined by law, and also captured by Internet systems and platforms, is used in a way that establishes a harm, resulting in economic inefficiency. For the purposes of this paper, anti-competitive behavior can be defined as personal data being harvested or mined, whether illegally or legally, to gain a dominant position in the market.

One of the problems is that the price effectively paid by consumers for Internet services now extends far beyond punctual advertising breaks (such as when using the music-streaming service, Spotify) or banner as flashing next to a search entry.[5] Data and search entries are often analyzed by data mining software that can result in various levels of intrusiveness, which in turn can create a system and environment whereby entities gain a competitive edge. The process of data mining provides the entity with specific information that a competitor who does not have the access or the systems and infrastructure to undertake the same activity – is at a disadvantage. It must also be noted that the collection, mining or harvesting of data may also provide many benefits to the consumer, for instance, improved services,[6] recommending certain products to the market or providing content that is free to the end user.[7]

Nevertheless, the data protection concerns specifically in relation to personal data are likely to remain because one of the most significant concerns arising from this behavior and practices is the rise in privacy breaches. Secondly, the privacy debate has also extended to difficulties for Internet users to be able to cope with privacy due to information problems and behavioral biases that have emerged. For instance, it is argued that users are intentionally kept uninformed or misled about the extent of the tracking of their behavior over the Internet. That

[3] M Stucke, A Grunes, *Big Data and Competition Policy* New York: Oxford University Press, (2016)
[4] A Bernasek, D Mongan, *"Our Massive New Monopolies: Amazon, Google and Facebook Have the Power to Move Entire Economies,"* Salon, (2015) https://www.salon.com/2015/06/07/our_massive_new_monopolies_amazon_google_and_facebook_have_the_power_to_move_entire_economies [accessed 22 June 2018].
[5] Organisation for Economic Co-operation and Development, Big Data: Bringing Competition Policy to the Digital Era, (2016), https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf, [accessed 5 August 2018].
[6] A Alessandro, H Varian, *Conditioning prices on purchase history*, Marketing Science (2005) 24(3): pp. 367–381.
[7] G Avi, C Tucker, *"Online Advertising."* In The Internet and Mobile Technology Advances in Computing, (2011) 81, pp. 290–337

tracking, to some degree, provides identifying data and information about the person. Moreover, people do not feel as though they have enough control over how their data is collected and specifically used by online platforms, systems and infrastructure.[8] When the data subject does not know how their data is collected and how the data holders may use that data, even the sophisticated consumer cannot protect themselves against these breaches.[9]

Wolfgang Kerber questions the extent to which secret collecting of data (through tracking with cookies and web bugs) should be prohibited, and if allowed, whether there should be a duty to informing users of a service or a website about the data collection?[10] By prohibiting the secret collecting, mining or harvesting of data, it is acknowledging that this activity amounts to the data being stolen. However, the answer may lie in what Kerber highlights as to the effectiveness of the concept of consent. Kerber argues that currently individuals, particularly across European Union (EU) member states, are informed about the "privacy policies", and implicitly consent to them by using the service, website or Internet platform. Effectively, the data subject provides a level of consent that their data can be collected, harvested or mined. Therefore, reinforcing the point that, where consent has not been obtained or granted for such an activity, the data is simply stolen.

Moreover, and apart from the traditional regulatory approach 'one group of solutions try to solve the problem of weak competition among Internet platforms in order to increase the incentives of the firms to offer their services in a more privacy-friendly way, for example, by being more responsive to the heterogeneous privacy preferences of their customers'.[11] The option of granting access to the already accumulated data of a dominant platform (as an essential facility) to other competitors for eliminating a huge entry barrier might admittedly help competition, but can be viewed critically from a privacy protection perspective due to further spreading private data.[12] To alleviate these competition concerns, it is argued that the right for data portability reduces switching costs that, in turn, lead to more competition between platforms, particularly in regard to social networks.[13] Furthermore, it is arguable that there is a link because of the singular power that the likes of Facebook and Google have, even though people can choose not to use them. However, with more and more of our daily lives being conducted over the Internet, the choice not to use these platforms continues to

[8] M Stucke, A Grunes, *Big Data and Competition Policy* New York: Oxford University Press, (2016).
[9] Wolfgang Kerber, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection*, No. 14-2016. Marburg Centre for Institutional Economics (MACIE), School of Business & Economics, Philipps-University Marburg (2018).
[10] Ibid. See also: EU ePrivacy Directive (2002/58/EC) and EU Cookie Directive (2009/136/EC) which permit the use of cookies if the users give their opt-in consent, whereas in the US the Do-not-track proposal of the FTC (Federal Trade Commission) in 2012 follows an opt-out approach. *FTC*, Protecting Consumer Privacy in an Era of Rapid Change, FTC Report March 2012, and for the EU *Luzak*, Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use in Order to Protect the Internet Users' *Right to Online Privacy, Journal of Consumer Policy* (2014) p. 547
[11] Ibid.
[12] Ibid.
[13] Ibid.

diminish. In effect everyone is slowly being directed to eventually use the Internet, and consequently these types of platforms. Therefore, the challenge is not only to determine the need for anti-competitive regulation, but also to combine that regulation with other regulation and non-regulatory mechanism to secure privacy, and ensure the right balance between these two regulatory regimes.

It is not within the scope of this paper to fully examine the theoretical concept of consent, except to acknowledge that it has emerged as a key concept in the data protection laws of the European Union (EU), Australia and Singapore. Consent provides individual data subjects with a level of control over their personal data that has been defined in law. It is argued that consent is conceived as being given at the moment at which personal information is exchanged. The ability to consent to the use of personal data in such circumstances has been limited, given that the party using the data is unknown to the data subject. This limitation is attributable to the fact that the data subject only ever provides consent to the data controller or data processor that sits within an entity.[14] The Organization for the Economic Co-operation and Development (OECD)[15] has identified this conception of consent as the key to strengthening the management, governance and regulation of data and privacy across all areas of law. Coupled with competition law, the concept of consent arguably has its challenges. Consent can come in the form of actual or implied consent, depending on the national or supranational laws. The question arises as to what actual personal data or personal information to which an individual is consenting to? That can only be found in data protection laws, such as the ones defined in Australia, the EU and Singapore.

Even though it is out of scope of this paper to examine the different definitions of personal data among the EU, Australia and Singapore, what is certain is that each jurisdiction has adopted a

[14] See Council Regulation (EU) 2016/679, General Data Protection Regulation, Article 7(4) affirms that the consent is not freely given if it is conditional. Article 6 requires that processing of personal data is to be lawful only if and to the extent that at least one of the following criteria applies: the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Consent in Australia is conceived broadly. There is no direct requirement or pre-requisite for collecting personal data or information from a data subject. However, for 'sensitive information' a person's consent must be provided. The Australian Privacy Principles (APPs) require that personal information should be collected directly from the individual, unless the individual has consented to collection from other sources, or if it is authorized by law. The APPs define consent as 'express consent or implied consent. Section 13 of Singapore's Personal Data Protection Act 2012, provides for a form of implied (deemed) consent, and prohibits organizations from collecting, using or disclosing an individual's personal data unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of personal data.

[15] Organization for the Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.ht m, [accessed 20 February 2018]. Organization for the Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.ht m, [accessed 20 February 2018].

slightly different approach.[16] Nevertheless, the question arises whether the current definition adequately captures all the relevant circumstances in which personal data is used to create anti–competitive environments? When related specifically to competition, the answer is clearly that further work is needed in this area of the law. What can be confirmed is the unlikelihood that personal data defined by the law includes all personal data that is captured, mined and harvested by Internet platforms. A notable exception is Article 4 of the General Data Protection Regulation (GDPR), which provides that a data subject can be identified either directly or indirectly.[17] By its very nature, the broad definition adopted by the GDPR does not specifically exclude the personal data that is captured by Internet platforms and infrastructure. The GDPR was only recently been implemented in May 2018, and is arguably the world benchmark in regulating individual's personal data. The principal aim of the GDPR is to provide data subjects with greater control over their personal data that has been defined by the law.

Similarly, section 2 of the Personal Data Protection Act 2012 states that personal data means data, whether true or not, about an individual who can be identified — from that data; or from that data and other information to which the organization has or is likely to have access. The courts in Singapore have reinforced this point. In *Re Executive Coach International Pte. Ltd,*[18] the Court concluded that the content of individuals' communications such as email messages and text messages, in and of themselves may not be considered personal data, unless they contain information about an individual that can identify the individual. Thus, it is argued that the court has expanded the definition of personal data to that which has been specifically provide for in the Personal Data Protection Act 2012. Likewise section 6 of the Australian Privacy Act 1988 defines personal information as information, or an opinion, about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether that information or opinion is recorded in a material form or not.[19] However, it is yet to be confirmed in Australia, particularly whether this definition would constitute the personal information which has been captured by Internet platforms and infrastructure. In other words, the courts in Australia have not yet handed down a decision confirming the scope and breadth of the definition of personal information.

This paper examines the interconnectedness between competition and data protection law. The paper also highlights current examples that have emerged in this area of law and includes the abuse of power by organizations to create a competitive edge, and how organizations, through mergers of companies and acquisition of entities, have been able to establish a dominant position through the acquisition and use of data.

[16] See Regulation (EU) 2016/679 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] OJ L 119/1, Article 4, sub (1).

[17] See General Data Protection Regulation, Official Journal of the European Union 2016/679, Article 4.

[18] [2017] SGPDPC 3.

[19] See Privacy Act 1988, section 6.

This paper proposes a two stage solution to the potential problems faced by the intersection between data protection (privacy) and anti-competitive behaviour. This paper explains how any personal data defined by law, which is stolen or used without the consent – is fully protected. On the other hand, personal data not defined by law has very little to no protection. To overcome some of the issues related to data protection and competition law, the paper will demonstrated how non-regulatory options through technology can assist in defining the intersection between anticompetitive behavior based on the misuse of personal data. The paper draws on experiences from the European Union, Australia and Singapore.

Data Protection and Competition

It is of value to understand the historical development in this area of law. Data protection and competition did not suddenly emerge, but developed over time. Arguably, the collection and use of personal data and data generally is now fast becoming an important part of the economy. The balance between data protection, particularly personal data which is defined the law and anti-competitive behavior, walks a thin line. That line becomes even more blurred when on the one hand governments do not want to stifle innovation, while on the other hand, data (commercial and personal) needs to be protected. Subsequently, there has been considerable debate as to whether a problem actually exists in the determining the relationship between personal data and anti-competitive behavior. That is, the nature of this relationship has never been clear, even in Europe which arguably is the leader in the development of data protection law. In 2006, the Court of Justice of the European Union made reference to the possible intersection between competition law and personal data, concluding that personal data, "*as such"*, was not a matter for competition law. At an early stage, the European Commission (EC) took the position that it refused to assess data protection in competition law cases. It was stated in Facebook/ WhatsApp that:

> *Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the European Union competition law rules but within the scope of the EU data protection rules.*[20]

This demonstrates the thinking at a time when technology was not significantly advanced. Thus, it took another 5 to 7 years before the general thinking in this area of law began to change. In 2013, the German and French competition authorities (*Bundeskartellamt* and the *Autorité de la Concurrenc* joint paper on *Competition Law and Data*' clearly acknowledged that, despite personal data concerns having specific laws at a supranational and national level, data protection laws did not preclude competition law from intervening. It was stated that the:

> "fact that some specific legal

[20] See *Case No COMP/M7217 - Facebook/ Whatsapp* [2014] European Commission Decision, para.165.

> instruments serve to resolve sensitive issues on personal data, it does not entail that competition law is irrelevant to personal data".[21]

Moreover, it was in 2015, when Alec Burnside summarized the interrelationship between data protection and antitrust (competition), from a privacy perspective. Burnside stated that:

> "(...) *It is hardly a blanket assertion that privacy is irrelevant to antitrust, or that antitrust must not address facts to which privacy laws may also be relevant. Rather, it indicates that antitrust rules should be applied in pursuit of antitrust goals. And indeed that is what the Court did in the case before it: apply the antitrust rules to a set of facts to which privacy disciplines had a parallel application*". [22]

Furthermore, in referring to the former European Commission for Competition, Margrethe Vestager, Burnside described personal data as the new currency of the Internet.[23] Privacy is a by-product of this new currency when traded according to applicable rules and laws. However, privacy becomes important when the data is harvested or mined illegally, heightening the potential to establish anti-competitive practices. What Burnside has been calling for is the need for antitrust law to evaluate the role of datasets when they arise in the factual matrix of any assessment, such as dominance, restrictive practices, or a merger review.[24] Therefore, it is argued that competition law cannot be set aside when a data set, of any size, contains personal data defined by the law, and is used to establish a dominant position.

This assessment is similar to that which has been espoused by Peter Wire[25] and Robert Lande[26]. Both seek to promote the need to undertake assessments of the potential or actual harm, choice and quality of the data that is being used to create an environment that would shut out any competitor.

Notwithstanding the above, if data about ourselves really is the price we pay for content and access to the Internet, why should competition law not limit a company's ability to

---

[21] See Autorité de la Concurrence and Bundeskartellamt, *'Competition Law and Data'*, p.23. *Case C-32/11 Allianz Hungária* [2013] Court of Justice of the European Union, ECLI:EU:C:2013:160, para. 46-47

[22] A Burnside, *'No Such Thing As A Free Search: Antitrust And The Pursuit Of Privacy Goals'* (2015) Competition Policy International, https://www.competitionpolicyinternational.com/assets/Uploads/BurnsideCPI-May-15.pdf, [accessed 4 August 2018].

[23] Ibid.

[24] Ibid.

[25] P Swire, *Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall*, (2007), http://ftc.gov/os/comments/behavioraladvertising/071018peterswire.pdf, [accessed 12 August 2018]. Peter Swire argues that the combination of deep and broad tracking resulting from the Google-DoubleClick merger is one example which goes some way to strengthening the protection of personal data. According to Swire, "this sort of quality reduction is a logical component of antitrust analysis [A]ntitrust regulators should expect to assess this sort of quality reduction as part of their overall analysis of a merger or dominant firm behavior.

[26] R Lande, *The Microsoft- Yahoo Merger: Yes, Privacy is an Antitrust Concern*, FTC: WATCH, (2008) p. 1. Lande argues that consumers also want an optimal level of variety, innovation, quality, and other forms of nonprice competition, including data protection.

collect and analyze that data?[27] At one level, there appears to be no issue with this concept, provided the data subject agrees to the collection and use of that data. On another level, this become very problematic because of the privacy issues related to the data obtained when there has been no agreement (consent) by the data subject. The resulting effect is a level of subjectivity, which is likely to deter data collection,[28] and which has mutual benefits for innovation and the economy more generally. James Cooper makes an important point that, in understanding data from a privacy perspective within the competition sphere, is not easy. Copper states:

> *We live in a world where a large portion of online content is free. We do not pay to search on Google or Bing, post our photos on Facebook or MySpace, or read the latest news on CNN.com or Foxnews.com. Apps like Angry Birds are available for free in Apple's and Google's app stores. Why does everyone give away things online? The answer, in some ways, is that they do not. These businesses ("publishers") monetize the content they provide for free by selling access to our attention. By collecting more data about their users, publishers can improve their products and target ads more precisely to the consumers who are most likely to respond.*[29]

Competition law can be appropriate where the potential harm is actual or potentially diminishing economic efficiency. In other words, anti-competitive behavior can be identified by the use of data or by the technology created to harvest the data. Attempting to unify competition and consumer protection laws creates needless risks for the Internet economy. In particular, it could destabilize the modern consensus on antitrust analysis, again pulling it away from rigorous, scientific and allegedly objective methods of such assessment developed in the last few decades, and reverting back to the influence of subjective noncompetitive factors. Indeed, trying to expand competition law, as some have proposed, better reflects legal thinking in 1915, not 2015. However, privacy can be (and is today) a dimension of competition, whereby the more direct route to protecting privacy as a norm lies in consumer protection laws.[30]

---

[27] J Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, George Mason University School of Law, (2015).

[28] Ibid.

[29] Ibid. Copper goes onto say that by doing more searches on Google - Google learns more about you. Combine your search data with what Google knows from your Gmail and other interactions with Google properties, as well as reports from tracking cookies placed by its display advertising network, and Google has a pretty good idea of what you like. Google can use this information to provide you with better search and map results, as well as more relevant ads, both of which will help Google's bottom line. First, better content makes for a more attractive product, encouraging greater use of Google's services, increasing both ad revenue and Google's database of consumer information. Second, the expansion of Google's database also allows Google to earn more revenue by facilitating targeted ads that are more likely to elicit consumer responses. see also Howard Beales, *The Value of Behavioral Targeting*, 1-2, 2010, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf, [accessed 29 August 2018].

[30] M Ohlhausen, A Okuliar, 'Competition, Consumer Protection, and The Right [Approach] to Privacy', 80 *Antitrust Law Journal* 121 (2015).

Maureen Ohlhausen and Alexander Okuliar in 2015 argued that privacy, as a result of entities obtaining personal data outside of the current legal framework, is part of a non-price dimension of competition that can hurt individuals in general, if some companies have too much market power.[31] What the authors are saying is that where there is too much market power, the possible resulting effect and impact could lead to a total reduction in data protection and subsequently privacy – in the absence of any regulation. Today, there are a number of countries that have either no or a limited regulatory framework for personal data. It is argued that competition law should look at data protection and subsequently privacy issues, even if no competitive implications exist. The authors go onto say that by rejecting attempts to incorporate data protection and privacy concerns into competition policy, three major problems emerge: 1) competition deals with harm to competition, not to privacy harms; 2) competition is concerned with market-wide effects, whereas privacy policy focuses on the individual relationship between the company and the consumer; and 3) competition remedies are inadequate to handle privacy concerns, specifically because companies can accomplish the same outcome through private contracts, rather than a merger.[32] However, when looking at this assumption closer, the authors are referring to data that has been obtained within the context of the law. That is, they have assumed that the data subjects have provided a level of consent for their data to form part of a contract within the confines of a merger. This assumption does not account for the data that has been illegally obtained (stolen), or where no contract or adequate level of consent has been provided.

In 2016, Germany and France released a white paper out of concerns raised in relation to market power and data. Firstly, the three broad areas of concern include, but are not limited to, the fact that the collection and exploitation of data may raise barriers to entry and may be a source of market power. Secondly, these barriers may reinforce market transparency, which may impact upon the functioning of the market. Thirdly, different types of data-related conduct relating to an undertaking might raise competition concerns.[33] Data can be obtained without consent to the user, through search engines and services including social networks, which use cookies and sensor data that track web surfing. The European Commissioner for Competition, in 2016, highlighted that:

> "*It's possible that in other cases, data could be an important factor in how a merger affects competition. A company might even buy up a rival just to get hold of its data, even though it hasn't yet managed to turn that data into money. We are therefore exploring whether we need to start looking at mergers with valuable data involved, even though the*

[31] Ibid, 134–36.
[32] Ibid.
[33] Competition Law and Data, Germany and France, White Paper, http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf, [accessed 17 December 2017].

company that owns it doesn't have a large turnover."[34]

In 2017, Inge Graef argued that both competition and data protection law are interlinked, even though they perform different functions.[35] Graef maintains that, ultimately, both sets of laws aim to protect consumer welfare,[36] by 1) regulating anticompetitive behavior and 2) ensuring an individual's privacy has a level of protection. Furthermore, the emergence of data analytics also poses challenges between competition and data protection law. Simply put, data analytics allow prediction of an individual's behavior over the Internet. This activity captures personal data that is both defined and not defined by the law, but can be used to identify an individual. The activity can transcend the economy and online shopping, to encompass health, education, recreational activities, sport preferences and even political or religious preferences. Not only will existing businesses be impacted by this behavior, but purported new entrants into the market may find themselves shut out because they cannot get access to the systems and data that creates this information.

More recently, Giuseppe Colangelo and Mariateresa Maggiolino have explored the interface between data protection and competition (anti-trust) law.[37] First, in an economy which data is collected in exchange for free services, low levels of privacy could be indicative of high levels of market power, including the harvesting of large amounts of data that are concentrated amongst a few dominant market entities. Secondly, it is considered that antitrust law can make up for the pitfalls of data protection law. The authors highlight that such pitfalls arise, for example, in considering whether a practice that renders a product less privacy-friendly could be considered to be anticompetitive, or whether antitrust law could intervene to protect privacy-enhancing technologies.[38] Giuseppe Colangelo and Mariateresa Maggiolino go onto to say that today it is increasingly more difficult to identify a competitive quantity of consumer data (the quantity of personal data that firms would naturally collect in competitive markets).[39] Whereas, in the analogue economy, the competitive level of the market price can be approximated by looking at marginal costs (or other measures of costs). However, in the fast growing digital economy, no one has quantified the benchmark for assessing the competitive quantity of personal data. Even data protection law cannot help in this regard because it only

[34] M Vestager, European Commissioner for Competition, '*Big Data and* Competition' (Speech at the EDPS-BEUC Conference on Big Data, Brussels) (2016), http://ec.europa.eu/commission/2014-2019/vestager/announcements/big-data-and-competition [accessed 29 July 2018].
[35] I Graef, 'Beyond Compliance: How Privacy And Competition Can Be Mutually Reinforcing', *Computers, Privacy & Data Protection Conference* (2017), https://www.youtube.com/watch?v=Af1qLye_-Ok, [accessed July 2018].
[36] Ibid.
[37] G Colangelo, M Maggiolino, Data Accumulation and the Privacy- Antitrust Interface: Insights from the *Facebook* case for the EU and the U.S. Transatlantic Technology Law Forum, Stanford Law School and the University of Vienna School of Law, (2018).
[38] Ibid.
[39] Ibid.

regulates the way in which personal data is collected, without addressing the quantities of personal data that individuals may transfer to entities.[40] Additionally, the value of personal data varies according to the data considered, which is also very hard to measure. Valuing data also does not lend itself to any form of inter-personal comparison, and cannot become a tool for measuring aggregated, or market, phenomena.[41]

In 2018, The Australian Competition and Consumer Commission released its Digital Platforms Inquiry – Issues Paper,[42] That paper raises concerns in relation to big data, including whether data platforms provide consumers with adequate levels of privacy and data protection. One of the major concerns has been the emerging issue related to the use of large sets of personal data being used for commercial purposes to enhance an entities' competitive position in the market.[43] The Issues Paper went onto say that using accumulating consumer behaviour data to expand targeted advertising may improve services to advertisers (and potentially be of greater interest to their audience), but also represents a cost to consumers in the form of a loss of privacy.[44] The Issue Paper also highlights how an increase in the level of personal data obtained from users or the supply of more data to third parties, is being viewed as an effective source of increasing the market price or in decreasing the quality of the 'free' service (e.g. social media interaction or search functionality) supplied to consumers.[45] Moreover, another potential source of concern is the extent to which consumers are aware of the amount of data they provide to digital platforms, the value of the data provided, and how that data is used.[46] This concern has arisen in Australia because consumers are required to provide wide-ranging consent regarding the collection and use of their data across a number of Internet platforms in ensure that they are supplied with adequate information on the data collection and in order to be able to secure informed consent in order to use the data.[47]

Over the past decade there has been a general shift and acknowledgment that competition and data protection law are interrelated, and no longer stand alone. These laws overlap, to some degree, because it is the data that is collected by Internet technologies that is used to establish a dominant position in the market. Furthermore, the interrelationship between competition and data protection laws is likely to become even more interconnected as technology evolves, and as larger quantities of personal and general data that

[40] Ibid. It must be observed that the above reasoning and the resulting link between market power and personal data has been elaborated, as previously stated, in relation to multi-sided media platforms, with the ultimate purpose of appreciating their market power. However, other tools and variables can be used to this end, such as: (i) the price of advertising space; (ii) the amount of advertising space imposed on users (i.e., the amount of users' attention required); and (iii) the quality of the "free" products and services.

[41] Ibid.

[42] Australian Competition and Consumer Commission, https://www.accc.gov.au/system/files/DPI%20-%20Issues%20Paper%20-%20Vers%20for%20Release%20-%2025%20F..%20%28006%29.pdf, [accessed 10 September 2018].

[43] Ibid, 9.

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] Ibid.

can identify individuals becomes more important as it generates ever larger economic activity.

What is at Issue & Potential Solution

The debate in relation to data protection and competition law is, arguably, complex and requires a balance that needs to be struck between the broader public benefit arising from a competitive market in personal data compared to the risk (breach of privacy) to a single individual or group. It is a global issue that requires a global response, beyond simply looking at individual national and regional responses. This is all on the backdrop of the perceived public benefit that has been derived from the Internet and its supporting systems, platforms and infrastructure. Furthermore, the balance between data protection and competition lie in what the current day laws provide.

It is well understood that economic scholars argue that restricting competition stifles innovation and change, which has broader economic impacts on the economy and society. Firstly, it must be noted that companies such as Google have provided a public benefit, by ensuring greater access to information, whether that is medical, personal, entertainment (sport and music) and legal. It can also be argued that Google and other Internet platforms have enhanced and changed the way people shop, interact and have access to justice. Without these innovations, societal change, as we know it today, would not exist. On the other hand, competition issues that have arisen from technological change alone have resulted in people's privacy being significantly reduced, and in many cases infringed. A good example was 2017-2018 when Cambridge Analytica had obtained large amounts of personal data and information of more than 50 million people.[48] Despite the privacy infringements, the data obtained was used generally for political purposes to gain a competitive edge. This example highlights how the mining and harvesting of personal data can be used in any area of the economy. The power of a single organization such as Facebook to collect and provide this volume of personal data had never been seen before. While most of the data was unlikely to be defined within the national or European data protection law, arguably there is likely to be elements that fall within the law. The broader issue is whether the personal data involved was stolen, or was it simply that individuals were misinformed. The question arises as to what level of consent, if any, was obtained from data subjects that their data could be used by Data Analytica? Clearly, the evidence suggests that Facebook was the original collector of the personal data.[49] The evidence also suggests that the action was undertaken by Facebook or Cambridge Analytica were without

[48] D Unterhalter, *Data privacy: why internet giants elicit antitrust critiques*, The Cambridge Analytica furore vindicates fear that groups such as Facebook are not benign monopolies, https://www.businesslive.co.za/bd/opinion/2018-04-18-data-privacy-why-internet-giants-elicit-antitrust-critiques, [accessed 22 June 2018].

[49] The actions taken by Cambridge Analytical resulted in the organisation harvesting and mining personal data of 50 million people unwittingly. The issues at hand was that there was no consent provided by any of the data subjects to which the personal data pertained, even though obtaining consent from 50 million people would be an enormous task.

the permission of the data subjects.[50] Thus, not only was there the potential for large scale breach of privacy, but the example demonstrates the ease with which an organization can obtain a competitive position, no matter what that market might be (c0mmercial or political).

Moreover, there is criticism by some that the introduction of the GDPR has not assisted. In fact, Swire and Lagos argue that Article 20 of the GDPR[51] has a perverse anti-competitive effect, because it applies broadly to various organizations, including those that currently hold a dominant position in the market.[52] Even though the rule pertains to data portability, which has been designed to promote competition, Swire and Lagos argue that it will ultimately come down to how the courts interpret and apply Article 20. They further highlight that an additional factor that also needs to be considered is how Article 20 will be enforced. Currently, there is no jurisprudence or scholarly argument that can direct or substantiate how Article 20 operates.[53] Yet, it is argued that Singapore in particular, by taking an economic approach to data protection, has been willing to minimize the effect of data protection and privacy on competition and innovation. Australia appears to have followed a similar path to Singapore, even though it is considered that Australia views privacy generally, not only economically, as a right to be protected.

The theory of harm, which is a well-established principle in competition law, poses further challenges when applied to anti-competitive practices that involve the use of data. Largely, it is an area that has not been fully tested, even though there is jurisprudence that has emerged in some jurisdictions, such as the EU. It is argued that, applying the harm test to competition matters involving data, would complement those other known harms such as the infringement to privacy. However, further work is required to better understand what and where the harm commences and concludes. Additionally, measuring the actual harm of an infringement of privacy will be challenging both economically and socially.

Regulatory

A potential way forward calls for more work to be undertaken to better understand the various approaches taken by different states in regulating competition, data protection and privacy. A starting point is the definition of personal data and personal information. There needs to be a comprehensive study undertaken to better understand whether this definition is adequate enough in relation to the extent to which personal

[50] Ibid.
[51] See Regulation (EU) 2016/679, Article 20 states, "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance (…)".
[52] P Swire, Y Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique", Maryland Law Review, Vol. 72, No. 2, (2013), http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3550&context=mlr, [accessed 6 August 2018].
[53] Ibid.

data and information can be collected by Internet platforms and systems. The study extend further to reconciling whether the definition is adequate to deal with future anti-competitive behavior. It appears that the EU and Singapore provide some clarification and certainty; however the position in Australia, at this current time, is less convincing and less certain.

Moreover, what is emerging is the importance of the role of consent has in individual's allowing entities to harvest and mine their personal data. As highlighted earlier in this paper, as Internet platforms continue to provide wide-ranging levels of consent, the boundaries of consent are unclear. Furthermore, the consent provided by data subjects for their data to be provided to and used by a third, fourth or even fifth parties and so on, appears to be under-informed at this level of abstraction. That is, Entity A has collected personal data from a data subject (X), who provides consent. Entity A then, under contract, provides Entity B, with that personal data to which the data subject did not consent. Entity B transfers the data to entity C, where no consent actually exists. Thus, unless Entity A clearly stated that upon consent from the data subject, Entity A can use the personal data in whichever manner they choose – consent from X has not been granted for Entity A or B to transfer or pass on X's personal data to Entity C and beyond. This is the unknown factor in most, if not all third party (and so on) transactions of personal data. This area of consent needs to be reconciled, both within the law and regarding the practical processes that better inform data subjects. This includes the personal data that are not defined by the law.

Over the past five years a number of issues have emerged in which the collection and use of both general and personal data has resulted in entities gaining a dominant position in a particular market. This is no more evident than in the areas of mergers and acquisitions. Section VI highlights an example from the EU, Australia and Singapore.

Types of Anti-Competitive Behavior - Mergers and Acquisitions [M&A]

One of the biggest issues facing the common market is the potential for monopolies to form through mergers and acquisitions with ease in the digital economy. The OECD reported that the number of mergers and acquisitions in the data sector had risen from 55 in 2008 to more than 160 in 2012.[54] M&As have two major challenges when it comes to data: first, the assumption that the merger or acquisition will be contrary to competition law; and second, the management and use of data, pre-contractually, on signing, and post contractually. Arguably, there is work to do to better understand this area of tension in the law. Yet, and while cases have emerged, such as those briefly discussed below, a settled position is far from being realized.

One of the largest acquisitions in the technology economy in recent times was WhatsApp by Facebook. The European

[54] Data-Driven Innovation: Big Data for Growth and Well-Being, OECD Publishing, Paris, 2015, http://dx.doi.org/10.1787/9789264229358-en, [accessed 17 June 2018].

Commission learnt that WhatsApp had begun to link its data with the data of Facebook. The resulting effect saw Facebook acquiring large amounts of personal data, it otherwise never available before. Even though, data, which formed part of the transaction did not really play a central role in determining whether a competitive advantage had been obtained, it is argued that, with data now being the new currency, some form of competitive advantage has been derived from this transaction. In other words, there are two ways whereby data that is used competitively arises through mergers, within the technology sector. It is either through the merging of entities, or in the context of privacy, as a non-price parameter that influences competition in the market. What is likely to be measured is the risk of harm from such a merger to the community and individuals. Subsequently, the European Commission fined Facebook €110 million for providing misleading information. Companies and businesses considering merging with, or, acquiring another company not only need to understand competition law, but also understand data protection law.

In another case, *Ryanair - Aer Lingus I*, the Commission built a theory of harm that included the quality of the service *ex post*, although price correlated. Firstly, quality was taken into consideration in the definition of the relevant market: it established a separation between 'full-service' (that offers a higher level of service) and 'low-frills' (low level of services that compete mainly on price) carriers. It found that the airlines offer low level of services, as Ryanair and Aer Lingus, still compete on quality, which it determined to be, for instance, their booking services or the routes and destinations to which they fly.[55] It was concluded that with Aer Lingus in the market - Ryanair might not have been able to decrease its prices, but it would still compete on quality. The merger was not approved. The take home message from this case in relation to personal data was in the use and application of the online booking system, by which airlines distinguished themselves from their competitors. It included a booking service (seat reservation, on-line check in and last-minute bookings), differentiation in services and prices for different types of customers. It also included unrestricted - flexible tickets, restricted roundtrip tickets, and customer loyalty schemes.[56]

In August 2017, Singapore undertook a whole of government analysis of data landscape in collaboration with Personal Data Protection Commission, Singapore ("PDPC"), and the Intellectual Property Office of Singapore ("IPOS"), to explore the implications of the proliferation of data analytics and data sharing on competition policy.[57] The reported noted that:

[55] See *Case COMP/M.4439Ryanair/Aer Lingus I* [2007] European Commission Decision, para. 38-49.
[56] Ibid. frequent flyer programs, services offered on the ground, free luggage handling, availability of a business lounge, free newspapers, in the air, availability of premium cabin classes, free drinks and food, number of crew, quality of the interior, or the destination airport such as "primary" airports close to city centres or more remote "secondary" airports.
[57] Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights, Intellectual Property Office of Singapore, Personal Data Protection Commission, Singapore

> 'The benefits arising from the adoption of data analytics and data sharing may not be fully realized if businesses engage in anti-competitive conduct in the course of adopting data analytics and/or data sharing. It is thus crucial for competition policy and law to foster a level playing field for businesses'.

The report concluded that 'while there have been calls for competition law to be applied to promote data protection and privacy policy, this is not consistent with the roles and functions of Competition Commission of Singapore (CCS). In this regard, CCS aims to ensure that markets are, and remain, competitive by protecting the competitive process. This extends to mergers and acquisitions, so that monopolies are not established from the acquisition and mergers of entities. Where data protection is a non-price competition factor, the treatment of personal data may affect how CCS considers and assesses the competitive dynamics of a market'.[58] This is an example of the recognition and balance that law and public policy has in a particular country. Arguably, Singapore will consider personal data, as a right to be protected in areas of consumer, competition and IP law. Although, Singapore is economically focused in how personal data is managed directed at retaining its reputation as a business-friendly environment.

Moreover, arguments over where and how data protection and competition issues might coexist has been highlighted by the former Federal Trade Commissioner, Pamela Jones Harbour.[59] Jones argued that mergers between companies that hold big data would, by increasing their joint data booty, allow the entity resulting from the merger to dominate the database of intentions by possessing even more tools for profiling individuals.[60] In addition, no firm is under an antitrust obligation to provide the absolute best quality product that it can, even if it does not maximize profits.[61] As a general matter, antitrust law does not intervene in relation to market features and structure. If network effects disincentive digital platforms from producing privacy-friendly services, then economic regulation, rather than antitrust law, should intervene.[62] However, antitrust law could intervene against a merger suppressing a privacy-enhancing technology, or against a boycott targeting the producers of privacy-friendly products-services.[63]

Notwithstanding the above, it is wrong to assume that once an M&A has concluded and signed off, personal data can be easily shared. There are different rules across different

16 August 2017, https://www.cccs.gov.sg/media-and-publications/publications/studies-research-papers/occasional-papers/data-engine-for-growth, [accessed 8 August 2018].

[58] Ibid.

[59] P.J. Harbour, Dissenting statement, In the matter of *Google/DoubleClick*, https://www.ftc.gov/sites/default/files/documents/public_statements/statement-mattergoogle/doubleclick/071220harbour_0.pdf , in Giuseppe Colangelo and Mariateresa Maggiolino, Data Accumulation and the Privacy- Antitrust Interface: Insights from the *Facebook* case for the EU and the U.S. Transatlantic Technology Law Forum, *Stanford Law School and the University of Vienna School of Law*, (2018).

[60] Ibid.

[61] Ibid.

[62] Ibid.

[63] Ibid.

countries, which is best to have sorted out in the pre-contractual and final contractual arrangements. Certain jurisdictions such as the EU have very specific rules governing the transfer of data to a third country that is outside the European Economic Area. Consent is one option in an M&A; however, an organization is likely to find it costly and time-consuming to deal with large quantities of data and information. The application of competition rules related to data protection will be commercial and private. Their formulation and application will encompass many other areas of law of which this article can only scratch the surface. Further research is this area is required. To mitigate against any breaches of data law, companies and businesses will need to understand the cross-border transfer effects of data laws. These laws vary from country to country. Nonetheless, this could be an area in which industry can regulate itself through effective contracts, data and risk management systems by ensuring the compatibility of data transfer from one system to another. However, as highlighted above, the competition issues arising from data transfers, are at best, still emerging and likely to continue to develop as continually changing and novel technology enter global markets.

Concluding Remarks

It is well understood that large-scale entities like Google and Facebook, along with many other companies, collect, collate and use people's personal data (both generally and defined by law), within their business model - to make profit from it. In some cases, those profits far exceed expectations from the business community and can about to millions, if not billions of dollars.

This paper has provided a glimpse of the issues and potential solutions to the tension between data protection and competition law. What is at issue is the ongoing need for regulator (s) to balance the economic needs of the country along with innovation and the protection of personal data and privacy. That balance is going to be continually challenged and may never be resolved. In other words, the balance between stifling innovation and protecting people's personal data and privacy, walks a thin line, because innovation is becoming increasingly dependent on large scale dissemination, transfer and trade in all forms of data, including personal data. This trade, not only heightens the potential for privacy breaches, but can also be used to obtain a market advantage.

Regulators are recognizing the importance of the interrelationship between personal data defined by law and general data that is being used by organization to create and establish a competitive advantage. Moreover, the 2018 GDPR establishes rules that provide citizens with greater control over their data through different mechanisms. These mechanisms include data protection by design, the right of notification in case of personal data breach, or by enhancing the power of data protection authorities to impose higher fines for breach comparably to those imposed by competition authorities. However, the GDPR does not solve, or adequately address the problem of not enforcing competition rules, given that Article 20 appears to have somewhat

confused the issue of enforcement. Moreover, it appears that the GDPR may actually impede competition by placing the data subject's rights to privacy at a higher level than that of the economic activity of the competitive entity purporting to use that data. Indeed, the converse appears to be the case in Singapore and Australia. However, the Australian Government is currently reviewing the impact of large scale mining, harvesting and collection of personal data from consumers.

The concept of consent and the definition of personal data and personal information have emerged as key to strengthening the interrelationship between competition, data protection and privacy law. Both the concept of consent and definition of personal data should not be seen as barriers to innovation or consumer protection. However, more work is needed to better prepare the community for the digital economy and potential competition issues that may arise. More work is required to better project and understand whether consent in its current form is adequate, along with understanding whether the definition of personal data or personal information (depending on the jurisdiction) meets current and future needs – particularly in relation to competition and data protection.

More work is also needed to better develop the theory and application of harm in relation to data protection and competition. What is certain, is the fact that personal data and data is being used to create anti-competitive environments. Unfortunately, however, the broader community is mostly unaware that this is occurring. This continued technological evolution and changes in technology are likely to make it even more challenging for data subjects to understand and measure the harm to them.

Australia and Singapore have currently entered a new phase of investigating into whether further regulation is needed in this area. But it remains to be seen whether these and other countries will be willing to harmonize their respective approaches over the longer term. Thus, the more pressing issue for countries such as Australia and Singapore, as well as the European Union, is the need to close gap between the policy objectives of competition and data protection. That is, the convergence of these laws are more likely than not to improve the balance between market forces, innovation and protecting people's personal data. The jury is out regarding the direction personal data and competition law will take, and where the balance between them will be settled. There are many unanswered questions because the area continues to evolve and change.

One way to resolve this is to conduct more in-depth analysis and research on data protection and competition in the immediate future. Different data protection and competition laws can achieve similar results, namely to protect the individual consumer, albeit in different ways and from different perspectives. Although there appears to be significant overlap between the objectives of these laws, they can arguably converge and be harmonized in the future to provide greater accountability to businesses, no matter what jurisdiction they are located. A starting point is for countries to set aside their different economic and social policies and objectives and work towards establishing a

balanced policy approach that would pave the way for legal harmonization. This approach can ensure that there is adequate competition in the new digital economy. Finally, the issues raised in this paper are not confined to a single nation state. Accordingly, the issues between competition and data protection law may also require an international response on a comparable basis to that proposed above in relation to the EU and the countries identified in the Asia-Pacific region.