PRIVACY AND DATA PROTECTION AS FACTORS IN COMPETITION REGULATION:

Surveying Competition Regulators to Improve Cross-Regulatory Collaboration

Digital Citizen and Consumer Working Group
Report to the 43rd Assembly of Authorities
October 2021

CONTENTS

EXECUTIVE SUMMARY

1. Since its inception, the Global Privacy Assembly's Digital Citizen and Consumer Working Group ("**DCCWG**") has been working to both better understand cross-regulatory intersections and actively promote cross-regulatory collaboration. The first two years were dedicated to studying the intersection between privacy, or data protection, and consumer protection, while the last two years have focused on the intersection of privacy and competition. Over the last four years, it has become increasingly apparent that these intersections will only continue to grow both in frequency and magnitude, as their interplay shapes today's digital economy and society.

2. This Report is the second report produced as part of our "Deep Dive" into the intersection of privacy and competition regulation. The first was the July 2021 release of *Digital Crossroads: The Interaction of Competition Law and Data Privacy*[1], an independent "academic review" commissioned by the DCCWG and authored by Professor Erika Douglas of Temple University, Beasley School of Law. Her report focused on an assessment of the complements and tensions created by privacy/data protection and competition agency mandates and objectives, as well as how competition authorities have accounted for privacy/data protection considerations when fulfilling their mandate. These two reports complement each other, bringing together both the theory and practical application underpinning our current understanding of this intersection.

3. Based on a series of competition authority interviews, this Report sets out to:

    i. Understand how the interviewed authorities are approaching privacy and data protection considerations when carrying out their competitive analyses; and

    ii. Leverage the views and examples provided to identify opportunities for greater collaboration between competition and privacy/data protection authorities.

    In the process, this Report provides expanded comments, analyses and opinion, in identifying and advocating for collaborative cross-regulatory opportunities.

4. The findings of this Report are split into three sections:

[1] *Digital Crossroads: The Interaction of Competition Law and Data Privacy*, by Professor Erika Douglas, 6 July 2021 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

i. "*Building a Shared Foundation*" explores some central concepts that will facilitate future cross-regulatory discussions and collaboration, including:

   i. The "traditionalist" approach to competition regulation, which postulates that authorities can better achieve their objectives by focusing on their own regulatory spheres. However, the growing incidence of privacy as a non-price factor in competitive assessments, represents an opportunity if not necessity, for greater collaboration – even with adherents to this regulatory approach;

   ii. The core mechanics underpinning competitive assessments. Ultimately, privacy will be relevant where it is an element of competition. By sharing their asymmetrical knowledge on privacy and data-driven models, privacy authorities can assist in strengthening the accuracy and predictive power of the potential competitive impacts of privacy and data-related factors;

   iii. The potential for artificial intelligence to facilitate anti-competitive conduct, and how a shared interest in this area represents an opportunity for authorities from both spheres to learn from each other and better understand this nascent technology; and

   iv. Examining how the data being shared in competition remedies allows privacy authorities to gain a better understanding of the competitive nature of that data, while competition agencies can gain a better understanding of potential privacy impacts and whether the shared data is in fact personal information.

ii. *"Moving Forward Together"* explores challenges to be addressed and practical examples of how competition enforcement has already incorporated privacy considerations, including:

   i. How we are speaking different languages across regulatory spheres. Ensuring that we understand each other is the first step to effective collaboration;

   ii. The importance of avoiding "either-or" outcomes that benefit one regime at the expense of the other and how the UK's Digital Regulation Cooperation Forum can serve as an example of how to mitigate against such outcomes towards supporting a robust digital economy;

iii. Taking a closer look at the Privacy Paradox, and exploring how it may be the result of a market failure driven by poor privacy related communications as well as default settings and choice architecture all of which favour the commercial interests of the business, rather than facilitating genuine consumer engagement and choice;

iv. Exploring how the difficulties associated with assigning a value and weight to privacy as a competitive factor represents an opportunity for privacy and data protection authorities to assist competition authorities in gaining a better understanding of privacy preferences and their associated implications; and

v. Presenting actual enforcement actions as practical and progressive examples of how agencies have already applied data protection and privacy considerations in fulfilling their mandates. In the process, we touch on the development of new competition enforcement guidelines, approaching privacy and data protection as both the cause of and justification for anti-competitive conduct in two different litigated matters, as well as two competition remedies that successfully balanced sharing personal information for competitive purposes with protecting privacy interests.

iii. *"Insights from the Digital Crossroads"* highlights three overarching themes identified by Professor Douglas that are similarly reflected in this Report:

i. That "antitrust and data privacy law are meeting in complex and multi-faceted ways, particularly in the digital economy";[2]

ii. The notion that "theory and practice at this frontier of the law are at an early stage" whereby practical examples remain "quite new, and present significant opportunities for development";[3] and

[2] See Erika Douglas, "*Digital Crossroads: The Interaction of Competition Law and Data Privacy"*, Report to the Global Privacy Assembly, DCCWG, 2021, at pg. 3. - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737
[3] *Digital Crossroads: The Interaction of Competition Law and Data Privacy*, by Professor Erika Douglas, 6 July 2021 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

iii. The sentiment that "data protection and antitrust authorities can no longer achieve their goals in isolation".[4] Since authorities share "common policy interests" as well as an ultimate goal of "benefitting consumers", cooperation on developing "cohesive, effective enforcement strategies" is paramount.

5. It is our belief that the insights and examples raised in this Report will support authorities from both regulatory spheres in gaining a better practical understanding of how they can approach, and improve, their cross-regulatory interactions. As you will see, one common theme throughout our interviews, is that collaboration and communications across regulatory spheres can only serve to improve outcomes for global citizens. It is our hope that this Report will serve as one of the early steps towards realizing those improved outcomes.

INTRODUCTION

THE GLOBAL PRIVACY ASSEMBLY'S DIGITAL CITIZEN AND CONSUMER WORKING GROUP

6. The Digital Citizen and Consumer Working Group ("**DCCWG**") was born from the recognition that "as privacy and data protection becomes an increasingly material factor of consideration for individuals as consumers, there has been a growing intersection of consumer protection, data protection and privacy issues, especially online".[5] The September 2017 *Resolution on Collaboration Between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy* adopted by the International Conference of Data Protection and Privacy Commissioners, now known as the Global Privacy Assembly, resulted in the DCCWG first exploring the intersection of privacy and consumer protection. In addition to promoting and encouraging cross-regulatory collaboration, the DCCWG conducted an in-depth study of the intersection of privacy and consumer protection

[4] *Digital Crossroads: The Interaction of Competition Law and Data Privacy*, by Professor Erika Douglas, 6 July 2021 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

[5] International Conference of Data Protection and Privacy Commissioners: *Resolution on Collaboration between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy*, 26-27 September 2017, Hong Kong - http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-collaboration-on-consumer-protection.pdf

and published a White Paper as part of its 2018 DCCWG Annual Report presented to the Assembly in Brussels, Belgium.[6]

7. As evidenced by our White Paper, and validated by the ever growing intersectional examples we have recorded,[7] the overlap between privacy and consumer protection is relatively well established and observed. With privacy and consumer protection more naturally aligned, it is not uncommon for the same harmful, deceptive, or misleading privacy practices to also raise consumer protection concerns (e.g. consent through deception), eliciting enforcement action under both regulatory regimes. Privacy continues to emerge as a material factor in consumer purchasing decisions and organizations are increasingly operating on this premise.

8. It was on this premise, that the DCCWG's focus has shifted to considering competition/anti-trust.[8] Research into the generally more complex relationship between the intersection of privacy and competition has led to a number of important outputs, including, this Report and its independent academic companion *Digital Crossroads: The Interaction of Competition Law and Data Privacy* ("**Digital Crossroads**")[9] by Professor Erika Douglas or Temple University, Beasley School of Law.

---

[6] *Digital Citizen and Consumer Working Group Report* on Collaboration between Data protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy - http://globalprivacyassembly.org/wp-content/uploads/2019/11/DCCWG-Report-Albania-2011014.pdf.

[7] As outlined in '*Annex 2 – Mapping of regulatory intersections and actual collaborative actions table*' of the DCCWG's 2020 Annual Report, examples include: 1/ the Philippines National Privacy Commission issuing a *Public Health Emergency Bulleting as Guidance for Establishments on the Proper Handling of Customer and Visitor Information for Contract Tracing* in July 2020; 2/ the Office of the Australian Information Commissioner contributing to a Joint Directory of Online Safety and Security Services with the Australian Competition and Consumer Commission, the Australian e-Safety Commissioner and the Australian Cyber Security Centre in June 2020; and 3/ the Norwegian Datatilsynet and the Norwegian Consumer Authority jointly developing and publishing a guide on digital services and consumer personal data that aims to help business operators, developers, marketers and providers of digital services navigate practical issues where consumer protection and privacy issues overlap in February 2020

[8] Most notably the International Conference of Data Protection & Privacy Commissioners unanimously adopted the DCCWG's resolution in 2019: *Resolution to Support and Facilitate Regulatory Co-operation between Data Protection Authorities and Consumer Protection and Competition Authorities to Achieve Clear and Consistently High Standards of Data Protection in the Digital Economy* - http://globalprivacyassembly.org/wp-content/uploads/2019/11/DCCWG-Resolution_ADOPTED.pdf

[9] *Digital Crossroads: The Interaction of Competition Law and Data Privacy*, by Professor Erika Douglas, 6 July 2021 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

CURRENT TRENDS IN THE DIGITAL ECONOMY: REGULATORY INTERSECTIONS IN PRIVACY AND COMPETITION

9. Like consumer protection, the intersection between privacy and competition is rooted in the digital economy and its growth and innovation. The emergence and morphing of data-driven business models has led to value being extracted from data more successfully than ever. Factors such as the monetization of personal information has contributed to data being made available on an unprecedented level, not only to dominant, global social and commercial enterprises, but also to small and medium-sized businesses. As the digital economy continues to evolve from the bricks and mortar world, so too have the competitive implications arising from the conduct of its players. Recognizing that data does not conform to regulatory boundaries, the privacy, or data protection, implications of companies amassing and using vast amounts of personal data has become more prominent than ever.

10. The digital economy has thrust the privacy/data protection and competition regulatory spheres together in ways not previously explored or fully understood. In the process, this intersection would currently appear to present as many regulatory complements as tensions. Arguably, all authorities, regardless of regime, find themselves at an inflection point on the way forward, as they develop strategies on how best to address regulatory intersections. Such challenges and dynamism have come into sharper focus in 2020/21 owing to the pandemic, which has driven increased consumer, business and societal reliance on all things digital. It is with this in mind that we set out to better understand how the intersection of privacy/data protection and competition is playing out in theory and in practice.

OBJECTIVES OF THIS REPORT

11. This report is the result of a series of interviews with competition authorities across the globe. This Report sets out to:

    i. Understand how the interviewed competition authorities are approaching privacy and data protection considerations when carrying out their anti-trust analyses; and

    ii. Leverage the views and examples provided to identify opportunities for greater collaboration between competition and privacy/data protection authorities.

12. This Report is presented in four parts. The first sets out the methodology underpinning the interviews and this Report. The second provides an overview of broader interview observations, while the third part provides specific examples of common themes and practical enforcement actions discussed during the interviews. Finally, the fourth part compares certain of our interview observations with the themes explored in the *Digital Crossroads* report.

PART 1 – METHODOLOGY

13. The DCCWG envisioned the development of complementary reports as part of a broader "Deep Dive" into the intersection of privacy and competition regulation.

14. The first report was the previously released *Digital Crossroads*, an independent "academic review" commissioned by the DCCWG and authored by Professor Erika Douglas. *Digital Crossroads* focused on an assessment of the complements and tensions created by privacy/data protection and competition agency mandates and objectives, as well as how competition authorities have accounted for privacy/data protection considerations when fulfilling their mandate. In the process, *Digital* Crossroads also identifies numerous examples of existing, and opportunities for further, collaboration across regulatory spheres.

15. In a complementary fashion, Professor Douglas explores the theory underpinning this intersection in considerably more detail in her *Digital Crossroads* report. This Report will leverage certain of the observations and analyses from *Digital Crossroads*, in considering the perspectives of interviewed competition authorities.

16. This Report constitutes the second component of the DCCWG's Deep Dive into the intersection of privacy and competition regulation. Where the *Digital Crossroads* represents independent academic research, this Report reflects the perspectives and practical realities faced by competition authorities when carrying out their day-to-day work. To this end, as described below, this Report relies on a series of competition authority interviews. It is our hope that when considered together, these reports will inspire longer-term focus on this intersection and present practical areas where privacy and competition authorities can collaborate. Such collaboration will enable authorities to work towards better understanding the interplay

between regulatory spheres and producing superior privacy and competition outcomes for global citizens.

17. This Report commenced with the development of a questionnaire, to ensure consistency between interviews. The questionnaire touched on:

    i. operational metrics of the agency being interviewed;

    ii. whether and to what extent they took privacy into account as part of their merger, abuse of dominance and general market power assessments;

    iii. practical examples of how privacy/data protection has factored into their work; and

    iv. cross-regulatory collaboration.

    DCCWG members then approached their competition counterparts and invited them to participate in an interview. At the same time, the Colombian Superintendencia de Industria y Comercio ("**SIC**"), whose mandate includes both privacy and competition (among others), asked some of its competition partners to participate in an interview.

18. All efforts were made to conduct in-person interviews via video conference. Alternatively, competition authorities were able to submit written responses to the questionnaire.

19. The interview teams were comprised of members of the Office of the Privacy Commissioner of Canada , or the SIC, or a combination of the two agencies. Generally, the in-person interviews were conducted in three person teams – with one person leading the interview and the others taking notes and occasionally framing follow-up questions. These interviews were fluid in nature and while they addressed all of the items in the questionnaire, they did not strictly adhere to the exact wording or sequence of each question. Rather, they followed the flow of the discussion and occasionally segued into items of interest and relevance beyond the questionnaire itself.

20. 12 interviews were conducted with the following agencies:

    i. Australian Competition and Consumer Commission

    ii. Autoriteit Consument & Markt (Netherlands)

    iii. Bundeskartellamt (Germany)

iv. Comisión Federal de Competencia Económica (COFECE) (Mexico)

v. Comisión Para Promover la Competencia (Costa Rica)

vi. Competition and Consumer Commission of Singapore

vii. Competition and Markets Authority (United Kingdom)

viii. Competition Bureau Canada

ix. Autoridad de Fiscalización de Empresas del Ministerio de Desarrollo Productivo y Economía Plural (Bolivia)

x. Federal Trade Commission (United States of America)

xi. Konkurrence og forbrugerstyrelsen (Denmark)

xii. Superintendencia de Industria y Comercio (Colombia)

21. Of the 12 agencies interviewed, the vast majority have a dual competition and consumer protection mandate. Two agencies are responsible for competition, consumer protection and privacy. Notably, while one authority has limited competition responsibilities, they are currently operating in a jurisdiction that does not yet have a dedicated consumer protection, competition or privacy authority. At the same time, several of the agencies are also responsible for fulfilling additional regulatory mandates above and beyond competition and consumer protection.

22. The interview responses were assessed to identify both general and specific insights for inclusion in this Report. This Report is not attempting to reproduce interview responses verbatim or in their entirety. Instead, it presents and expands upon identified overarching and recurring themes, while also presenting practical examples of, or opinions regarding, cross-regulatory cooperation.

23. Finally, note that in alignment with the mandate of the DCCWG to facilitate cross-regulatory cooperation, this Report provides expanded comments, analyses and opinion, in identifying and advocating for collaborative opportunities. While this Report is primarily for a privacy audience, it will introduce certain foundational competition related concepts, as opposed to engaging in a substantive discussion around competition theory. At the same time, while “privacy” and “data protection” carry different meanings, in recognition of the fact that regardless of their title these

authorities are both working towards the same objectives, this Report will use the two terms interchangeably.

24. As noted in *Digital Crossroads*, we remain in the very early days of understanding the intersection of privacy and competition. It is the DCCWG's belief that authorities can work together across both spheres to realize responsive enforcement that will readily adapt to tomorrow's business practices, and ultimately ensure a more holistic and superior outcome for the protection of both privacy rights and consumer interests in the process. It is the DCCWG's hope that this Report and its companion, *Digital Crossroads*, will help pave the way forward.

PART 2 – BUILDING A SHARED FOUNDATION

25. Intersections between privacy and competition are a fairly recent phenomenon. While all interviewed agencies were able to comment on the challenges and opportunities, not all were able to point to examples of how this intersection has materialized in practice. The earliest example identified during the interviews came from the US Federal Trade Commission ("**US FTC**"), noting one Commissioner's 2007 Dissenting Statement on the Google/DoubleClick merger, which argued that "without imposing any conditions on the merger, neither the competition nor the privacy interests of consumers will have been adequately addressed."[10] With the exception of one other example dating back to 2014, the other examples cited in the interviews (and discussed below in '*Part 3 – Moving Forward Together*') tended to have occurred within the last few years.

26. Before going further, it is worth acknowledging the reality that certain jurisdictions do not have a full complement of consumer protection, competition or privacy authorities (either separately or under multi-mandated authorities). Work carried out by the DCCWG, and a comparable project undertaken by the International Competition Network,[11] will lead to greater cross-regulatory awareness and facilitate strategies for taking advantage of complements and

[10] In the matter of Google/DoubleClick F.T.C. File No. 071-0170, Dissenting Statement of Commissioner Pamela Jones Harbour, pg. 1 – https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf

[11] Scoping paper – Competition law enforcement at the intersection between competition, consumer protection, and privacy. Paper for ICN Steering Group (2020) - https://www.internationalcompetitionnetwork.org/wp-content/uploads/2020/05/SG-Project-comp-cp-priv-scoping-paper.pdf

mitigating tensions between competition and privacy. However, we cannot lose sight of the fact that not all jurisdictions have the same comprehensive or balanced level of regulatory protections in these areas. Competition laws are more historically entrenched (some tracing back over a hundred years) than the recent adoption of privacy laws in various jurisdictions. When a lack of coverage exists, it generally involves the existence of a competition law but an absence of privacy laws and/or regulators. This evolving regulatory landscape represents an opportunity, where new authorities are coming online, for the creation of better-integrated regimes from the outset – ones with collaboration and cross-regulatory cooperation built into their foundations as opposed to seeking to incorporate and adopt collaborative strategies within already established regimes.

27. Turning to the central theme of the intersection between competition and privacy regulation, references were made by several interviewees to the continued support and validation for a "traditionalist" approach to regulation. This is not to say that a majority of agencies advocated for this approach, but rather recognizes that this was a topic of discussion during agency interviews and was identified as an evolving debate within the broader competition community. This approach is rooted in the view that competition authorities can more effectively achieve their mandates by focusing on competitive issues and elements when assessing the conduct at issue, and setting aside any factors that do not have a competitive bearing on the conduct. Under this theory, competitive assessments utilize traditional competitive indicators such as price or market share, and would generally exclude factors such as privacy. Certain proponents of this approach to regulation view different regulatory spheres as having been created for a reason, and that authorities ought to focus their energies within the four corners of their mandate, trusting that other authorities will similarly address any ancillary problems within their regulatory spheres. In other words, competition authorities regulate competition and should leave privacy-related issues to privacy authorities.

28. The debate around this approach is considerably more complex and nuanced than this Report is able to explore. However, this Report still advocates for the benefits of cross-regulatory collaboration, even within such an approach. Specifically, data protection considerations would factor into such analyses where they represent a bona fide competitive factor (e.g., where two merging entities are competing on the degree of privacy protection provided to customers). As will be touched on further in this Report, this represents an opportunity for competition

authorities to collaborate with privacy authorities, who enjoy a comparative advantage with respect to knowledge of how certain privacy functions operate, towards improving the level of statistical confidence in anti-trust analyses.

29. As noted in the introduction, all authorities, regardless of regime, are at an inflection point on the way forward, as they develop strategies on how best to address the dynamic growth and interconnected nature of the digital economy. The increased reliance on all things digital for businesses, societies and individuals, has brought both challenges and dynamism into sharper focus. From the rapid growth of video teleconferencing services in lieu of in-person gatherings to the explosion of retailers of all sizes developing new online platforms, Covid-19 has *driven the world indoors and online*. In the face of such a rapid and tectonic shift, this Report would argue that all authorities, not simply privacy and competition agencies, need to reassess their approach to the digital economy. This represents an opportunity to work together, where relevant and warranted, and ensure that we, as a community of regulators, are adequately addressing the realities of today's digital economy. Working together will help ensure that we, collectively, have a better understanding of the issues faced by each regulatory sphere, and will afford us the opportunity to develop a coherent strategy, based on that shared understanding. Specifically for the intersection of data protection and competition, this is an opportunity to help make better-informed decisions with respect to how the actions of one sphere may affect the other. With this in mind, this Report details below certain interview insights that are likely to help advance these discussions.

UNDERSTANDING THE MECHANICS BEHIND A COMPETITIVE ANALYSIS

30. As a starting point, we should consider the foundational regulatory objectives underpinning data privacy and competition regulation. Global data-driven companies being examined on anti-trust grounds are also being scrutinized with regard to privacy practices – but while both regulatory regimes may take an interest in the same company, the fundamental reasons for doing so originate from different departure points. Where privacy authorities are concerned with protecting individuals' privacy, competition authorities are looking to ensure healthy competitive economies and properly functioning markets.

31. Competition authorities' competitive assessments are both anchored in, and bounded by, economic theory and practice. Anti-trust analyses look to assess the competitive impacts of the

conduct at issue. To this end, if privacy is not a direct or peripheral element of the competitive conduct at issue, it is not automatically a relevant factor of consideration – regardless of how much personal information a party may hold. For example, let us take a hypothetical merger between a company that makes widgets and one that makes fitness trackers. The fact that the widget company will gain access to all of the personal information held by the fitness tracker company would not be of concern to a competition authority because there is no competitive overlap between the two companies. In contrast, privacy would become a relevant factor to that authority when assessing a merger of two fitness tracker manufacturers who actively compete in the level of privacy afforded to users (e.g., where one attracts users because of their increased privacy protections, while the other attracts users because of their overwhelming market presence).

32. Similarly, the fact that many privacy jurisdictions and authorities deem privacy to be a fundamental human right does not automatically elevate privacy's value in competitive assessments. As was noted in one interview, deeming something a right does not translate into practical guidance on how that right is to be applied in different regulatory settings. A concern and challenge expressed during the interviews was that privacy considerations are inherently difficult to assess for a variety of reasons (a few of which will be discussed below in greater detail), and simply accepting that "privacy is a right" does little, if anything, to help competition authorities overcome those difficulties and assign privacy a value and/or weighting in competitive assessments.

33. A related item raised in two interviews was the fact that competition agencies are still in the early analytical stages of assessing the market power impacts of combined data sets post-merger. Such impact assessments can be further complicated by the challenges associated with evaluating new and/or different types of digital market transactions and novel anti-competitive conduct that competition agencies are not accustomed to dealing with. Armed with minimal precedential material, it is difficult to assess the full impact of such conduct from the outset.

34. This has led certain governments to enact legislation to enable more effective analysis of the development of digital markets and their implications for economic competition. For example, the government of Mexico amended the statute for its Comisión Federal de Competencia Económica ("**COFECE**") in 2020 to establish a *General Directorate of Digital Markets*. Amongst other responsibilities, the Directorate is tasked with monitoring the development of digital

markets in which users' personal data becomes a variable to effective competition, from both a company-to-company and company-to-user perspective.

35. The challenges outlined above present collaborative opportunities where privacy authorities may possess an asymmetric knowledge advantage regarding digital market data-uses and the dynamics underpinning privacy considerations overall. In this scenario, collaboration with privacy authorities to harness their experiences could assist in strengthening the accuracy and predictive power of competition authorities' assessments of the competitive impact(s) of privacy and data-related factors.[12]

DATA MAY FACILITATE TOMORROW'S ANTI-COMPETITIVE CONDUCT

36. Turning to data-centric innovations, we heard that present day practical realities of how companies are leveraging personal data and employing technological innovations may bring the journey between theory and practice into sharper focus. The US FTC interview was the first of two interviews to flag and articulate the growing potential for artificial intelligence ("**AI**"), an area of clear interest in the realm of data protection, to facilitate anti-competitive conduct. With price being a key component in competitive analyses, a series of questions to be asked is whether, with the use of AI, a company can:

    i. Increase the price after a merger;

    ii. Use its dominant position to keep prices so low that others cannot compete; or

    iii. Collude with other companies to artificially increase the price of a product.

37. It is this last question where the US FTC explained that AI holds the theoretical potential to support collusion, whether tacit or intentional. For example, let us assume that **company A** develops an AI algorithm to track price fluctuations across the market and to help them set their prices. At the same time, **company B**, **company A**'s primary competitor, deploys a similar algorithm. In its simplest form, this creates a situation where the two algorithms, interacting with the same data universe, can essentially "learn from each other" and in order to maximize profits, arrive at the same artificially inflated price. While alarming and a logical extension of a

[12] The idea of privacy regulator expertise being valuable to competitive assessments is also a thread throughout the *Digital Crossroads*

self-learning, profit-maximizing AI system in theory, neither of the agencies raising the prospect were aware of it yet happening in practice. The other agency was of the view that, in today's technological environment, this idea is interesting but currently a theoretical possibility.

38. Given the automated and "self-learning" nature of such scenarios, AI can become even more insidious and difficult to detect, when driven by AI systems that facilitate personalized pricing or analyze user habits in online marketplaces. In both instances, the "price setting" algorithms can evolve from making decisions based on publicly advertised prices to decisions based on real world practices and discriminating pricing models targeting individual consumers, where there are potential privacy implications.

39. Regardless of whether such risks may arise as described above or in some other mutated form, given data protection and competition authorities' independent yet concurrent focus on AI's effect on either privacy rights or competition, they can only benefit by pooling resources and sharing knowledge and expertise in dealing with AI-related enforcement or policy endeavors.

THE NATURE OF DATA BEING SHARED IN A COMPETITIVE REMEDY

40. Remedies to prevent market power in mergers or to restore competition in markets with dominant players arose in multiple interviews as situations where a tension between competition and privacy objectives can manifest. For example, where a merger remedy contemplates data-sharing with other market participants, the sharing of data with market players outside the merged entity can very well enhance, or preserve, competition. Conversely, the broader sharing of data and personal information can diminish individuals' privacy rights.

41. However, what we also heard is that such an apparent conflict does not mean that solutions cannot be found that serve, or respect, both regulatory objectives. For example, Mexico's COFECE highlighted an example of an investigation it had conducted, which determined that a dominant player in the credit reporting industry should be sanctioned for refusing to share basic customer information with its competitors. COFECE found that in denying access to financial information generated by its customers, the dominant player effectively created a barrier to entry to the credit information market. COFECE further stated that while legislation regulating credit reporting companies stipulates that companies must share a base minimum of user information sufficient to develop basic financial products, detailed information can only be shared by credit reporting companies for a regulated price and with a client's consent. This

protects consumer data while still providing new competing companies with access to a guaranteed minimum amount of user data.

42. The interview with the United Kingdom's Competition and Markets Authority ("**CMA**") led to valuable insights with respect to the construction of competitive remedies that require data sharing. In short, it was suggested that there was value in recognizing the nature of the data that companies are looking to receive when data sharing forms part of a potential competitive remedy. To this end, they pointed to the potentially less privacy intrusive situation where, to restore competition (or prevent an exercise of market power), third-party competitors are provided access to broader search patterns/trends, foregoing any need to share actual personal information about the users conducting those searches.

43. Such considerations begin to take on more importance as multiple jurisdictions move towards establishing and/or entrenching data portability rules. Allowing consumers to take their data with them will clearly have an impact on both competition and privacy. Being able to easily switch between competing service providers will drive companies to continually assess whether their products, services or prices remain attractive to existing and perspective clients. At the same time, the transfer of customer data between competitors has to be done in a manner that ensures the protection of personal information.

44. Recognizing that context is key, it is again believed that both data protection and competition authorities can benefit from broader discussions about the type(s) of information being shared in competitive remedies. Privacy authorities can gain a better understanding of the competitive nature of this data, while competition agencies can gain a better understanding of both the privacy impacts and whether the shared data is in fact personal information. Ideally, a solution can be found that achieves both competitive objectives, while also respecting privacy rights. For an excellent illustration of balancing to achieve such an outcome, see the Australian and Colombian examples as described below in '*Successfully Balancing Privacy and Competition*'.

PART 3 – MOVING FORWARD TOGETHER

45. The interview team also gained a variety of specific insights into:

    i. How, and the extent to which, competition agencies have approached the incorporation of data protection into their enforcement efforts; and

    ii. The current state of cross-regulatory cooperation.

46. A number of these insights were common across the interviews. The following provides some specific examples to highlight where competition agencies have been able to incorporate privacy factors, or undertaken practical collaboration.

WE ARE SPEAKING DIFFERENT LANGUAGES

47. The first of these insights came into focus during the interview with the Competition Bureau Canada, and became evident across almost all other interviews - privacy and competition authorities speak different regulatory languages with varied interpretations of certain concepts. Our interview questionnaire referred to how "privacy" was factored into anti-trust analyses. Interviewees understandably addressed the question by considering how companies may compete on the basis of "privacy protection", that being, how "privacy" impacts competition between companies. However, when the discussion evolved to the role of "data", or "personal information" in merger analyses, we often heard a very different set of examples and theories. In short, as privacy authorities, the interview team instinctively treated the concepts of personal information and data under the same broad conceptual umbrella of "privacy" during the initial agency interviews. However, the interviewee interpreted these terms differently and they carried different competitive implications. As a basic example, two merging firms may not compete on the basis of the privacy protections they offer their customers (thus making privacy irrelevant to their analyses), however the merged data-set may confer market power on the merged entity (making data highly relevant).

48. A first principle in being able to collaborate productively is to ensure that we understand one another. While not necessarily advocating for the development of a new privacy/competition lexicon, it is helpful for authorities to understand the nuanced meanings of mutually relevant terms. Where privacy speaks of terms such as user consent, anonymization and publicly

available information, competition concerns itself with market power, pricing and non-price factors, as well as barriers to entry. Privacy authorities focus on "personal information" or "personal data" (depending on an agency's preferred terminology), while competition authorities tend to focus on "data" more generally (potentially personal and/or not personal) as one of multiple elements to determine a relevant product market.

49. Given the economic lens adopted by competition agencies, privacy authorities may generally be unfamiliar with the concept of a "relevant product market" – a technical term for identifying all of the products/services that a consumer would find interchangeable. For example, a product market could be comprised of: air travel, lending services, or mid-size cars. More privacy related, product markets could include social network platforms or search engines. Consideration is also given to the relevant geographic markets for the products (domestic, global, etc.) Finally, competition agencies focus on the degree of competition in such product and geographic markets and whether market power exists through dominant players, or would exist if proposed mergers were to be allowed.

50. Just as privacy authorities are likely not familiar with relevant product markets, it is equally unlikely that competition authorities are familiar with the privacy concepts of accountability or openness. Regardless of how concepts translate from one sphere to the other, there is mutual value in ensuring a basic understanding of what each other is saying. As authorities engage further, it will be important for each to take the time to articulate the meaning of key concepts. The development of a "cross-regulatory glossary" of key terms may in fact prove a worthwhile endeavor to this end.

COLLABORATION TO AVOID "EITHER-OR" OUTCOMES

51. Perspectives shared in the interview with the United Kingdom's Competition and Markets Authority served as one example of how authorities have confronted the misconception of an irreconcilable dichotomy of "good for privacy" and "bad for competition", and vice versa. Differing mandates and objectives sometimes cause authorities to move or peer in opposite directions. Data sharing stands as an illustrative example. From a privacy perspective, the unauthorized use and sharing of personal information generally runs counter to privacy rights. From a competitive perspective, limiting access to user data can negatively affect competition or act as a barrier to entry to a market for new competitors.

52. As noted by the CMA and other agencies interviewed, sharing information with other market participants can mitigate the market power of a dominant market participant. Depending on your specific approach to data sharing, fulfilling your privacy obligations could create competition concerns, while a competition remedy that involves data sharing can infringe on privacy rights. As previously noted, the challenge is finding a common middle ground between both regulatory spheres that protects both privacy and competition without harming either – all while continuing to develop and support a robust digital economy.

53. Towards achieving complementary outcomes that support the digital economy in the UK, the CMA is a member of the recently established Digital Regulation Cooperation Forum ("**DRCF**"). The DRCF was formed in July 2020, publishing its priorities and workplan in March 2021.[13] The overarching goal of the DRCF is for participating authorities to better respond to the scale and global nature of large digital platforms and the speed at which they innovate. Comprised of the CMA, the Information Commissioner's Office ("**ICO**"), the Office of Communications (or Ofcom) and the Financial Conduct Authority (joining in April 2021), the DRCF hopes to leverage increased cross-regulatory cooperation in order to support a more coherent and coordinated digital regulatory approach. As noted in the DRCF's 2021-2022 work plan, "[g]reater coordination can both support each regulator in meeting these challenges [posed by digital regulation] in their own remit and ensure that we are able to provide a coherent approach to regulation for both industry and individuals."[14] The DRCF is a prime example of how authorities can increase cross-regulatory cooperation while fulfilling their respective enforcement mandates, via strategic and formalized network engagement.

54. While not raised in the CMA interview (as it had not been released at the time), an example of how the DCRF can serve as a model of increased competition and privacy authority collaboration can be found in the *Competition and data projection in digital markets: a joint statement*

[13] *Digital Regulation Cooperation Forum: Plan of work for 2021 to 2022*, 10 March 2021 - https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022

[14] *Digital Regulation Cooperation Forum: Plan of work for 2021 to 2022*, 10 March 2021 - https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022

between the CMA and the ICO issued in May 2021. As an extension of both agencies' DRCF work, the joint statement addresses key areas of their future collaboration such as:

- the important role that data – including personal data – plays within the digital economy
- the strong synergies that exist between the aims of competition and data protection
- the ways that the 2 regulators will work collaboratively together to overcome any perceived tensions between their objectives
- practical examples of how the 2 organizations are already working together to deliver positive outcomes for consumers[15]

55. By addressing digital economy risks in a coordinated fashion, the DRCF can help consumers make more informed, better choices, as it relates to purchasing decisions or privacy rights. In fact, it is reasonable to assume that consumers would intuitively expect coordination by their regulators.

56. The DRCF and the CMA/ICO's joint statement are but two examples of how competition and privacy regulation can leverage regulatory overlap or proximity, and work together to the benefit of consumers and the digital economy in general.

THE "PRIVACY PARADOX" AS A MARKET FAILURE

57. One recurring theme that came up in several interviews was the difficulties associated with trying to assign a value to personal information/data when treating privacy as a non-price factor in a competitive assessment. Often when the subject came up, it was accompanied by reference to the Privacy Paradox, which proposes that *while individuals claim to value their privacy, their actions suggest otherwise*. Regardless of the rationale behind such behaviour, it does underscore the complex nature of assessing a value for privacy as a non-price competitive factor.

58. The CMA suggested that the Privacy Paradox might really be a by-product of corporations' lack of privacy engagement with individuals, as opposed to the expression of an individual preference (or lack thereof). In essence, it was proposed that many companies are choosing to do the bare minimum to comply with privacy regulations as opposed to meaningfully engage with their customers with respect to their privacy practices and options. They may not be

[15] *Competition and data protection in digital markets: a joint statement between the CMA and the ICO*, 19 May 2021 - https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law

applying the same level of care and effort to ensuring customer engagement with their privacy communications as they do with other forms of customer communications, such as their corporate websites or social media presence.

59. Companies will continually monitor and assess how their customers interact with corporate websites or social media posts, and where these interactions are deemed insufficient or problematic, companies will identify the problematic elements and redesign/re-calibrate how they engage their customers as appropriate. The CMA proposed that the same level of care and responsiveness does not appear to be applied to privacy communications. Corporate privacy communications appear driven by regulatory obligation rather than a genuine desire to ensure customer understanding. Instead of developing concise, easy to understand policies that individuals can readily digest they present individuals with long, technical and complex privacy policies that would require consumers to translate them into plain language, in order to truly understand the privacy implications and make an "informed" decision about whether to share their personal information. Companies may also use default settings or choice architecture, which favour the commercial interests of the business, rather than allow genuine engagement and choice.

60. It was further submitted that, instead of enabling a free and informed choice, the practical effect of these frictions and choice barriers is to drive individuals to simply click "accept" in order to obtain the desired product or service. This perspective is consistent with consumer choice and demand-side distortion arguments noted in *Digital Crossroads*.[16]

61. Such views and perspectives resonated with members of the DCCWG's interview team. While the existence of some level of Privacy Paradox is widely accepted, its *cause* is clearly up for debate. In considering causal relations, it would appear a considerable leap in logic to conclude that people sharing their information equates to not caring about their privacy. This would represent a pretty significant case of group denial where *everyone answers the opposite of what they feel*.

[16] See Part 1, subsection 4(c), *'Consumer Choice and the Challenges of Demand-Side Distortions'* in *Digital Crossroads: The Interaction of Competition Law and Data Privacy*, by Professor Erika Douglas, 6 July 2021 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

62. Rather, we would suggest that the idea of a Privacy Paradox may be rooted in part in a misunderstanding about what privacy actually means, where some incorrectly equate privacy with secrecy, rather than *control* over one's personal information, and how/when individuals choose to share it (i.e., the exercise of freedom). People may be willing to share their personal information for specific purposes, but that does not mean that they do not care how their information will be used or disclosed. For example, they may click 'yes' to location tracking so that their food delivery app gets their pizza to their table on time, but do so without realizing that their personal information will be shared with third-parties for advertising purposes.

63. Turning the paradox question around and approaching it from a market perspective, we believe the following questions could be posed:

    i. Is the paradox not more likely an indication of market failure?

    ii. Has gathering and processing all of the relevant privacy information become so onerous and time-consuming for consumers that instead of deciding whether they are comfortable sharing that information they simply give up and accept anything just to get through the transaction and use the service?

64. Such questions raise yet another opportunity for collaboration between privacy and competition authorities. Regardless of reasoning underpinning the Privacy Paradox, be it that consumers answer the opposite of what they feel or whether it is driven by a market failure, we note the parallels to the wide variety of *price* preferences across multiple markets and how those preferences have successfully been incorporated into competitive analyses. Studying and appreciating the true nature of the Privacy Paradox can assist competitive assessments by competition agencies, and specifically, with understanding how demand for privacy should be accurately modeled in anti-trust analyses. Should this phenomenon truly be a market failure, the possibility of increased consumer engagement by businesses could help close the gap between consumers stated concern for privacy and how they act on those concerns, which in turn might make it easier for competition authorities to measure the competitive impacts of privacy as a non-price factor.

PRIVACY AS A COMPETITIVE ENIGMA (RATHER THAN A PARADOX)

65. Regardless of the causes, as we heard from the US FTC, the fact that individuals have a wide spectrum of privacy preferences only serves to complicate efforts to assess the competitive impacts of privacy. The complexities with obtaining a clear, or consistent, picture of consumer privacy preferences translates into comparable challenges in weighing the impact of privacy on competition.

66. It is not simply a question of whether privacy will be lessened, but whether privacy is an element of competition *and* whether the conduct at issue will ultimately lessen or prevent competition overall. As the market does not always reveal consumer privacy preferences, in lieu of assessing privacy, competition regulators may instead have to turn to alternative proxies or more qualified considerations, making it harder to identify and accurately quantify the competitive privacy implications along the way. A concept that arose in multiple interviews is that it is harder to identify and assess privacy as a competitive factor (be it an increase or decrease in privacy protections, or privacy as an aspect of product quality) than it is to identify and assess a more traditional competition concept like a price increase or decrease. A secondary challenge here is the risk of incorrectly imposing a privacy value judgement on a market where privacy may not actually have a competitive impact.

67. Again, this represents another opportunity for greater collaboration between competition and data protection authorities. While privacy will not always be a factor in competition, when it is, privacy authorities are well positioned to help contextualize how privacy may be valued or measured. By building a greater understanding of privacy preferences, competition agencies will be able to more easily identify associated implications across a wider range of competitive assessments, leading to better results for all.

COMPETITION ENFORCEMENT THAT INCORPORATES PRIVACY CONSIDERATIONS

68. Over the course of the agency interviews, several agencies shared the various approaches that they had taken to incorporate privacy considerations into the fulfillment of their mandates. This has taken the shape of offering guidance on how privacy might factor into competitive assessments, taking advantage of cross-regulatory opportunities with negotiated settlements, challenging the notion that privacy considerations justify anti-competitive conduct, or outright arguing that privacy practices can constitute anti-competitive conduct.

OFFERING GUIDANCE ON PRIVACY AS A COMPETITIVE FACTOR

69. On the policy front, the interview with the Competition and Consumer Commission of Singapore ("**CCCS**") revealed actions taken in the area of enforcement guidelines. The interview team learned that in September 2020, the CCCS launched a public consultation on proposed amendments to its *Guidelines on the Competition Act (Cap. 50B)*, which among other things, specifically identified data protection as an aspect of competition on quality that may be taken into consideration in its merger assessments.[17] Recognizing the importance of the control or ownership of data, the CCCS also proposed amendments to the CCCS *Guidelines on the Section 47 Prohibition*, in respect of the abuse of dominance, to clarify that the CCCS may consider other determinants of competition such as the control or ownership of data in assessing market power. The proposed amendments also clarified that the refusal by a "dominant undertaking" to provide access to key inputs such as physical assets, proprietary rights or data may constitute an abuse of dominance. The CCCS's revised Competition Guidelines have not yet been published at the time of preparing this Report. Overall, this development in Singapore points directly to the manners in which data protection can factor into anti-trust analyses. It also further underscores the noted collaborative opportunity for competition authorities to consult with data protection/privacy authorities given the latter's expertise and comparative advantage in this area.

PRIVACY HAS BEEN A SWORD AND SHIELD IN COMPETITION ENFORCEMENT

70. Where many interviews involved competition agencies discussing hypothetical instances of privacy as an element of competition, two agencies also provided case examples of how privacy became a central issue in their enforcement efforts. Two abuse of dominance cases initiated by Germany's Bundeskartellamt ("**BKartA**") and the Competition Bureau Canada (the **"CBC**"), respectively, have seen privacy presented as both the cause of, and justification for, anti-competitive conduct.

71. As described in the BKartA's written interview responses, they viewed privacy, among other considerations, as a sword against anti-competitive conduct:

[17] *Public Consultation on Proposed Changes to Competition Guidelines* - https://www.cccs.gov.sg/public-register-and-consultation/public-consultation-items/2020-public-consultation-on-proposed-changes-to-competition-guidelines?type=public_consultation

> The German Facebook case is a prominent example in which privacy considerations were relevant for the Bundeskartellamt's finding of an abusive practice. Among other conditions, private use of the network is subject to Facebook being able to collect an almost unlimited amount of any type of user data from off-site-sources, allocate these to the users' Facebook accounts and use them for numerous data processing purposes. Third-party sources include Facebook-owned services such as Instagram or WhatsApp, but also third-party websites which include interfaces such as the "Like" or "Share" buttons.
>
> The Bundeskartellamt found that Facebook's terms of service and the manner and extent to which it collects and uses data amount to an abuse of dominance. In assessing the appropriateness of Facebook's behaviour under competition law[,] the Bundeskartellamt had regard to the violation of the European data protection rules to the detriment of users. **Our authority closely cooperated with data protection authorities in clarifying the data protection issues involved**.
>
> …
>
> The Bundeskartellamt's decision is not yet final; Facebook has appealed the decision. [Emphasis added]

72. In an earlier matter, the CBC successfully completed litigation against the Toronto Real Estate Board ("**TREB**"). Where the BKartA viewed privacy as a sword, TREB unsuccessfully used Canada's private sector privacy legislation as a shield in an attempt to justify what the courts found to be anti-competitive conduct. The CBC's case focused on the restrictions TREB imposed on its members' use and online disclosure of certain important data in the Multiple Listings Service (a database of both current property listings and historical sales data), including preventing that data from being displayed online through virtual office websites. "The … [CBC] alleged that TREB's restrictions limited the impact of new and innovative business models and services that were a competitive threat to TREB members who preferred to compete using more traditional business models." [18] In defending their restrictions, TREB argued that they "were designed to protect consumer privacy to comply with federal privacy law and requirements of the provincial real estate regulator."[19]

73. Ultimately the Canadian Competition Tribunal rejected TREB's privacy defense and in response to TREB's appeal, the Canadian Federal Court of Appeal upheld the Tribunal's decision and found that that:

[18] Backgrounder: Abuse of dominance by the Toronto Real Estate Board - https://www.canada.ca/en/competition-bureau/news/2018/08/backgrounder-abuse-of-dominance-by-the-toronto-real-estate-board.html
[19] Backgrounder: Abuse of dominance by the Toronto Real Estate Board - https://www.canada.ca/en/competition-bureau/news/2018/08/backgrounder-abuse-of-dominance-by-the-toronto-real-estate-board.html

> [131] In considering privacy as a business justification under paragraph 79(1)(*b*), the Tribunal found that the **'principal motivation in implementing the VOW [virtual office websites] Restrictions was to insulate its members from the disruptive competition** that [motivated] Internet-based brokerages' (TR at para. 430). **It concluded that there was little evidentiary support for the contention that the restrictions were motivated by privacy concerns** of TREB's clients. The Tribunal also found scant evidence that, in the development of the VOW Policy, the VOW committee had considered, been motivated by, or acted upon privacy considerations (TR at para. 321). **The privacy concerns were 'an afterthought and continue to be a pretext** for TREB's adoption and maintenance of the VOW Restrictions' (TR at para. 390). …
>
> [146] However, earlier in its reasons, the Tribunal wrote that 'legal considerations, such as privacy laws, [may] legitimately justify an impugned practice, provided that the evidence supports that the impugned conduct was primarily motivated by such considerations' (TR at para. 294). …
>
> [147] This does not, however, eliminate the burden of the corporation to establish a factual and legal nexus between that which the statute or regulation requires and the impugned policy.[20] [Emphasis added]

74. While the Canadian courts rejected TREB's privacy arguments, they also left the door open to the possibility of privacy legislation justifying otherwise anti-competitive conduct – provided a company has sufficient evidence to support such an argument.

SUCCESSFULLY BALANCING COMPETITION AND PRIVACY

75. It is clear that one of the overriding challenges with the intersection of privacy and competition regulation is finding a balance between the two. Achieving such a balance represents a clear objective of collaboration amongst authorities, or within individual authorities (i.e., where privacy and competition are enforced by the same agency). Where avoidable, competitive markets should not come at the expense of diminished privacy protections, nor should data protections come at the expense of reduced competition and consumer welfare. It is with this in mind that we turn to two examples of competition agencies looking beyond the strict confines of their mandate and successfully incorporating privacy considerations into their competition remedies.

76. The first example comes from the Australian Competition and Consumer Commission ("**ACCC**") and the August 2018 Transurban Undertaking in relation to the then-proposed acquisition of a

[20] Toronto Real Estate Board v. Commissioner of Competition, 2017-12-01, Federal Court of Appeal Docket: A-174-16, Citation: 2017 FCA 236 – https://decisions.fca-caf.gc.ca/fca-caf/decisions/en/item/301595/index.do

majority interest in the WestConnex motorway. The ACCC was concerned in part that traffic data not generally available to others gave Transurban a competitive advantage over firms who face barriers to competing successfully for toll road concessions. To address these concerns, the ACCC sought a remedial undertaking where "the objective of the Transurban undertaking … [was] to provide other bidders who compete for future toll road concessions in NSW [New South Wales] with access to traffic count data that Transurban Group has as a result of its extensive interests in toll road concessions".[21]

77. Recognizing that where parties undertake to share data to address competition concerns, it must be done within the boundaries of the relevant privacy laws, the ACCC accepted the Undertaking offered by Transurban. The Undertaking is drafted in such a way that Transurban is not obliged to publish data where it would cause it to be in breach of "Privacy Obligations" as defined in the Undertaking.[22]

78. The second example comes from Colombia's Superintendencia de Industria y Comercio's assessment of the creation of a new digital joint venture between Bancolombia S.A., Banco Davivienda S.A. and Banco de Bogotá S.A. (collectively the "**Banks**") and the SIC's corresponding recommendations to the Superintendencia Financiera de Colombia (Colombia's financial regulator). The digital joint venture saw Colombia's three largest banks form a new company ("**NewCo**") to provide digital identification services in support of the financial services the Banks provided to their customers.

79. As with the US FTC and as noted above, the SIC has multiple enforcement mandates, including consumer protection, competition and privacy. Recognizing the privacy implications that this digital joint venture represented, and the need for the joint venture to garner consumer trust in its services through transparency and respect for Colombia's privacy regulations, the team assessing the Banks' proposal consulted with their privacy counterparts on what privacy considerations should be included in the SIC's recommendations. To that end, despite the competitive nature of the assessment, several of the SIC's recommendations were privacy-oriented. Such recommendations included:

[21] https://www.accc.gov.au/public-registers/undertakings-registers/transurban-limited
[22] Clause 5.11 of the Transurban Undertaking to the Australian Competition and Consumer Commission - https://www.accc.gov.au/system/files/public-registers/undertaking/Transurban%20Limited%20s87B%20undertaking%20%28redacted%29.pdf

i. Ensuring customer data was treated in accordance with Colombia's privacy laws;

ii. Only transferring customer data to NewCo if the Banks obtained customer's express consent to do so; and

iii. Allowing for data portability should new entrants create competing platforms.[23]

80. The Australian and Colombian examples illustrate how a balance can be realized between the two regulatory spheres with carefully developed remedies informed by the interplay of privacy and competition factors. In both cases, they were able to achieve a pro-competitive outcome in a manner that did not sacrifice, and in fact preserved, privacy protections.

PART 4 – INSIGHTS FROM THE *DIGITAL CROSSROADS*

81. As part of the Deep Dive project, the DCCWG envisioned coupling the findings of this Report with an academic one, in order to provide an independent, scholarly examination and analysis of the intersection between the regulatory spheres of privacy and anti-trust/competition.

82. The *Digital Crossroads: The Interaction of Competition Law and Data Privacy*[24] report provides a richly detailed and timely explanation of our current intersectional regulatory landscape and the ways in which this intersection may evolve in the future. Designed with a privacy audience in mind, *Digital Crossroads* features an important primer on the main features of competition analysis, theoretical frameworks relevant to privacy as a factor in competition analysis as well as highly relevant examples and case studies that exemplify the complex relationship between the two regulatory spheres.

83. While these two reports touch on some of the same content, *Digital Crossroads* has highlighted three overarching themes for understanding the intersection of anti-trust law and data privacy

[23] (Banks assessment and recommendations) *Respuesta a solicitud de análisis de una operación de intefración empresarial entre* ***BANCOLOMBIA S.A., BANCO DAVIVIENDA S.A. Y BANCO DE BOGOTÁ S.A.***, pg. 18 – https://www.sic.gov.co/sites/default/files/files/integracion_empresarial/pdf/2019/julio/BANCOLOMBIA%20-%20DAVIVIENDA%20-%20BANCO%20DE%20BOGOT%c3%81.pdf

[24] *Digital Crossroads: The Interaction of Competition Law and Data Privacy*, by Professor Erika Douglas, 6 July 2021 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

that are similarly reflected in many of our broader findings. These are worth considering in further detail here.

84. First, *Digital Crossroads* highlights that "antitrust and data privacy law are meeting in complex and multi-faceted ways, particularly in the digital economy."[25] It continues by noting that the relationship between the two regulatory spheres is nuanced, with many interactions only beginning to be dependably understood. This theme is also broadly reflective of our interviews with competition authorities. While many authorities did not necessarily foresee these interactions occurring at such a rapid rate, nor had they comprehensively examined them in the course of their investigatory work, there was a general acknowledgment that these intersections are occurring and will need to be 'reckoned with' presently and in the future. Going back over a decade, the dissent in the US FTC's decision on the Google/Double-click merger certainly held a prescient reference to negative privacy impacts. And indeed, the CMA-ICO joint statement on competition and data protection law in the digital economy[26] represents an important acknowledgment that the intersections between these regulatory fields are not materializing in a vacuum.

85. The second theme presented in *Digital Crossroads* involves the notion that "theory and practice at this frontier of the law are at an early stage" whereby practical examples remain "quite new, and present significant opportunities for development."[27] This finding was consistently reflected in our interviews with competition authorities. Whether it be organizations that had not yet encountered the intersection in their day-to-day work or organizations who had only begun to hypothetically apply their current regulatory analysis to cross-regulatory considerations such as privacy, it is clear that much of the examination of this intersection is at a primordial stage. This new frontier provides an excellent opportunity for domestic and international collaboration to build knowledge, consensus and frameworks that might apply cross-jurisdictionally.

[25] *Digital Crossroads: The Interaction of Competition Law and Data Privacy*, by Professor Erika Douglas, 6 July 2021 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737
[26] CMA-ICO Joint Statement on Competition and Data Protection Law – https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law
[27] *Digital Crossroads: The Interaction of Competition Law and Data Privacy*, by Professor Erika Douglas, 6 July 2021 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

86. Finally, the last theme emphasized in *Digital Crossroads* concerns the sentiment that "data protection and antitrust authorities can no longer achieve their goals in isolation".[28] Since authorities share "common policy interests" as well as an ultimate goal of "benefitting consumers", cooperation on developing "cohesive, effective enforcement strategies" is paramount. In our agency interviews, there was a genuine appetite for strengthening collaborative efforts. While opinions varied as to whether or not competition law should be adapted to include privacy considerations in its contextual analysis of anticompetitive factors, there was broad support for dialogue and cooperation with domestic partners, as well as general support for the sharing of best practices and information with international partners and agencies. Even though some agencies were bound by domestic legislation limiting information sharing with international agencies/networks, there was still an eagerness to work together globally, through working groups and other international fora.

87. The themes articulated above provide a very brief glimpse of Professor Douglas' nuanced and thorough report, and how it aligns with our own takeaways from the agency interviews. We believe the *Digital Crossroads* report will function as a foundation on which to build our understanding of the intersection between data protection and competition. Most importantly, we emphasize the view that as instances of the intersection become more prominent, collaborative relations between authorities will be required in order to overcome any potential regulatory obstacles.

CONCLUSION

88. First and foremost, the DCCWG and the interview team for this Deep Dive project wish to express their appreciation for the participation of all competition authorities, and the valuable insights and perspectives shared.

89. It was truly evident that the interviewed authorities are taking a progressive and proactive approach in considering how privacy and data are to be factored into anti-trust analyses. Even in

[28] *Digital Crossroads: The Interaction of Competition Law and Data Privacy*, by Professor Erika Douglas, 6 July 2021 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

jurisdictions that are yet to have a privacy authority in place, there was an acknowledgement of the inevitability of privacy impacts when regulating data-driven markets.

90. We heard and understood that even with a more ”traditionalist” regulatory strategy, the incorporation of data protection considerations remain valuable and necessary, in particular where privacy or data considerations factor directly into the anti-trust calculus.

91. To the extent that privacy and data considerations are necessary in competitive analyses, collaboration and consultation with privacy authorities, who have an experiential advantage overseeing privacy/data protection, can assist competition authorities in improving the predictive value of the anti-trust assessments, particularly given challenges in the measurement of qualitative privacy-related factors that are less objective than traditional price/cost factors.

92. We also heard of collaborative models giving rise to more formal cooperation networks, with an overarching objective to support and build a robust digital economy and society, of which the furtherance of consumer interests and privacy rights are requisite component parts.

93. We further saw examples and cases where, notwithstanding the existence of tensions between regulatory objectives, consultation and cooperation can result in an outcome that satisfies both objectives, rather than sacrificing either.

94. The common theme that came through, regardless of form or scope, is that collaboration and communication across regulatory spheres can only serve to improve outcomes for global citizens. Such an exercise, considered in concert with the reflections of *Digital Crossroads*, serves to further validate a key mandate pillar of the DCCWG: promoting and facilitating cross-regulatory cooperation to the holistic benefit of the global constituents we serve.